# User Guide for Cisco Secure ACS for Windows Server

Version 3.3

May 2004

**Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7816592=
Text Part Number: 78-16592-01

Downloaded from www.Manualslib.com manuals search engine

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

*User Guide for Cisco Secure ACS for Windows Server*
Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Downloaded from www.Manualslib.com manuals search engine

# CONTENTS


**Preface** xxix

- Audience xxix
- Organization xxix
- Conventions xxxi
- Product Documentation xxxii
- Related Documentation xxxiii
- Obtaining Documentation xxxv
  - Cisco.com xxxvi
  - Ordering Documentation xxxvi
- Documentation Feedback xxxvi
- Obtaining Technical Assistance xxxvii
  - Cisco Technical Support Website xxxvii
  - Submitting a Service Request xxxvii
  - Definitions of Service Request Severity xxxviii
- Obtaining Additional Publications and Information xxxix

CHAPTER 1

**Overview** 1-1

- The Cisco Secure ACS Paradigm 1-2
- Cisco Secure ACS Specifications 1-3
  - System Performance Specifications 1-3
  - Cisco Secure ACS Windows Services 1-4
- AAA Server Functions and Concepts 1-5
  - Cisco Secure ACS and the AAA Client 1-6





Downloaded from www.Manualslib.com manuals search engine

AAA Protocols—TACACS+ and RADIUS 1-6
TACACS+ 1-7
RADIUS 1-7
Authentication 1-8
Authentication Considerations 1-9
Authentication and User Databases 1-10
Authentication Protocol-Database Compatibility 1-10
Passwords 1-11
Other Authentication-Related Features 1-16
Authorization 1-17
Max Sessions 1-18
Dynamic Usage Quotas 1-18
Shared Profile Components 1-19
Support for Cisco Device-Management Applications 1-19
Other Authorization-Related Features 1-21
Accounting 1-22
Other Accounting-Related Features 1-22
Administration 1-23
HTTP Port Allocation for Administrative Sessions 1-23
Network Device Groups 1-24
Other Administration-Related Features 1-24
Posture Validation 1-25
Cisco Secure ACS HTML Interface 1-25
About the Cisco Secure ACS HTML Interface 1-26
HTML Interface Security 1-26
HTML Interface Layout 1-27
Uniform Resource Locator for the HTML Interface 1-29
Network Environments and Administrative Sessions 1-30
Administrative Sessions and HTTP Proxy 1-30
Administrative Sessions through Firewalls 1-31



Downloaded from www.Manualslib.com manuals search engine

Administrative Sessions through a NAT Gateway 1-31
Accessing the HTML Interface 1-32
Logging Off the HTML Interface 1-33
Online Help and Online Documentation 1-33
Using Online Help 1-34
Using the Online Documentation 1-34

CHAPTER 2 **Deployment Considerations** 2-1
Basic Deployment Requirements for Cisco Secure ACS 2-2
System Requirements 2-2
Hardware Requirements 2-2
Operating System Requirements 2-2
Third-Party Software Requirements 2-3
Network and Port Requirements 2-4
Basic Deployment Factors for Cisco Secure ACS 2-6
Network Topology 2-6
Dial-Up Topology 2-6
Wireless Network 2-9
Remote Access using VPN 2-12
Remote Access Policy 2-14
Security Policy 2-15
Administrative Access Policy 2-15
Separation of Administrative and General Users 2-17
Database 2-18
Number of Users 2-18
Type of Database 2-18
Network Latency and Reliability 2-19
Suggested Deployment Sequence 2-19



Downloaded from www.Manualslib.com manuals search engine

CHAPTER 3 **Interface Configuration** 3-1

Interface Design Concepts 3-2
User-to-Group Relationship 3-2
Per-User or Per-Group Features 3-2
User Data Configuration Options 3-3
Defining New User Data Fields 3-3
Advanced Options 3-4
Setting Advanced Options for the Cisco Secure ACS User Interface 3-6
Protocol Configuration Options for TACACS+ 3-7
Setting Options for TACACS+ 3-9
Protocol Configuration Options for RADIUS 3-11
Setting Protocol Configuration Options for IETF RADIUS Attributes 3-16
Setting Protocol Configuration Options for Non-IETF RADIUS Attributes 3-17

CHAPTER 4 **Network Configuration** 4-1

About Network Configuration 4-1
About Distributed Systems 4-2
AAA Servers in Distributed Systems 4-3
Default Distributed System Settings 4-3
Proxy in Distributed Systems 4-4
Fallback on Failed Connection 4-5
Character String 4-6
Stripping 4-6
Proxy in an Enterprise 4-6
Remote Use of Accounting Packets 4-7
Other Features Enabled by System Distribution 4-8
Network Device Searches 4-8
Network Device Search Criteria 4-8
Searching for Network Devices 4-9



Downloaded from www.Manualslib.com manuals search engine

AAA Client Configuration 4-11
AAA Client Configuration Options 4-11
Adding a AAA Client 4-16
Editing a AAA Client 4-19
Deleting a AAA Client 4-21
AAA Server Configuration 4-21
AAA Server Configuration Options 4-22
Adding a AAA Server 4-24
Editing a AAA Server 4-26
Deleting a AAA Server 4-28
Network Device Group Configuration 4-28
Adding a Network Device Group 4-29
Assigning an Unassigned AAA Client or AAA Server to an NDG 4-30
Reassigning a AAA Client or AAA Server to an NDG 4-31
Renaming a Network Device Group 4-32
Deleting a Network Device Group 4-32
Proxy Distribution Table Configuration 4-34
About the Proxy Distribution Table 4-34
Adding a New Proxy Distribution Table Entry 4-35
Sorting the Character String Match Order of Distribution Entries 4-36
Editing a Proxy Distribution Table Entry 4-37
Deleting a Proxy Distribution Table Entry 4-38

CHAPTER 5 **Shared Profile Components** 5-1
About Shared Profile Components 5-1
Network Access Filters 5-2
About Network Access Filters 5-2
Adding a Network Access Filter 5-3
Editing a Network Access Filter 5-5



Downloaded from www.Manualslib.com manuals search engine

Deleting a Network Access Filter 5-7
Downloadable IP ACLs 5-7
About Downloadable IP ACLs 5-8
Adding a Downloadable IP ACL 5-10
Editing a Downloadable IP ACL 5-13
Deleting a Downloadable IP ACL 5-14
Network Access Restrictions 5-14
About Network Access Restrictions 5-15
About IP-based NAR Filters 5-17
About Non-IP-based NAR Filters 5-18
Adding a Shared Network Access Restriction 5-19
Editing a Shared Network Access Restriction 5-23
Deleting a Shared Network Access Restriction 5-24
Command Authorization Sets 5-25
About Command Authorization Sets 5-26
Command Authorization Sets Description 5-26
Command Authorization Sets Assignment 5-28
Case Sensitivity and Command Authorization 5-29
Arguments and Command Authorization 5-29
About Pattern Matching 5-30
Adding a Command Authorization Set 5-31
Editing a Command Authorization Set 5-33
Deleting a Command Authorization Set 5-35

CHAPTER 6 **User Group Management** 6-1
About User Group Setup Features and Functions 6-2
Default Group 6-2
Group TACACS+ Settings 6-2



Downloaded from www.Manualslib.com manuals search engine

Basic User Group Settings 6-3
Group Disablement 6-4
Enabling VoIP Support for a User Group 6-4
Setting Default Time-of-Day Access for a User Group 6-5
Setting Callback Options for a User Group 6-7
Setting Network Access Restrictions for a User Group 6-8
Setting Max Sessions for a User Group 6-12
Setting Usage Quotas for a User Group 6-14
Configuration-specific User Group Settings 6-16
Setting Token Card Settings for a User Group 6-18
Setting Enable Privilege Options for a User Group 6-19
Enabling Password Aging for the CiscoSecure User Database 6-21
Enabling Password Aging for Users in Windows Databases 6-26
Setting IP Address Assignment Method for a User Group 6-28
Assigning a Downloadable IP ACL to a Group 6-30
Configuring TACACS+ Settings for a User Group 6-31
Configuring a Shell Command Authorization Set for a User Group 6-33
Configuring a PIX Command Authorization Set for a User Group 6-35
Configuring Device-Management Command Authorization for a User Group 6-37
Configuring IETF RADIUS Settings for a User Group 6-38
Configuring Cisco IOS/PIX RADIUS Settings for a User Group 6-40
Configuring Cisco Aironet RADIUS Settings for a User Group 6-41
Configuring Ascend RADIUS Settings for a User Group 6-43
Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group 6-44
Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group 6-46
Configuring Microsoft RADIUS Settings for a User Group 6-47
Configuring Nortel RADIUS Settings for a User Group 6-49
Configuring Juniper RADIUS Settings for a User Group 6-50



Downloaded from www.Manualslib.com manuals search engine

Configuring BBSM RADIUS Settings for a User Group 6-51
Configuring Custom RADIUS VSA Settings for a User Group 6-53
Group Setting Management 6-54
Listing Users in a User Group 6-54
Resetting Usage Quota Counters for a User Group 6-55
Renaming a User Group 6-55
Saving Changes to User Group Settings 6-56

CHAPTER 7 User Management 7-1
About User Setup Features and Functions 7-1
About User Databases 7-2
Basic User Setup Options 7-3
Adding a Basic User Account 7-4
Setting Supplementary User Information 7-6
Setting a Separate CHAP/MS-CHAP/ARAP Password 7-7
Assigning a User to a Group 7-8
Setting User Callback Option 7-9
Assigning a User to a Client IP Address 7-10
Setting Network Access Restrictions for a User 7-11
Setting Max Sessions Options for a User 7-16
Setting User Usage Quotas Options 7-18
Setting Options for User Account Disablement 7-20
Assigning a Downloadable IP ACL to a User 7-21
Advanced User Authentication Settings 7-22
TACACS+ Settings (User) 7-23
Configuring TACACS+ Settings for a User 7-24
Configuring a Shell Command Authorization Set for a User 7-26
Configuring a PIX Command Authorization Set for a User 7-29



Downloaded from www.Manualslib.com manuals search engine

Configuring Device-Management Command Authorization for a User 7-30
Configuring the Unknown Service Setting for a User 7-32
Advanced TACACS+ Settings (User) 7-33
Setting Enable Privilege Options for a User 7-33
Setting TACACS+ Enable Password Options for a User 7-35
Setting TACACS+ Outbound Password for a User 7-37
RADIUS Attributes 7-37
Setting IETF RADIUS Parameters for a User 7-38
Setting Cisco IOS/PIX RADIUS Parameters for a User 7-39
Setting Cisco Aironet RADIUS Parameters for a User 7-41
Setting Ascend RADIUS Parameters for a User 7-43
Setting Cisco VPN 3000 Concentrator RADIUS Parameters for a User 7-44
Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User 7-46
Setting Microsoft RADIUS Parameters for a User 7-47
Setting Nortel RADIUS Parameters for a User 7-49
Setting Juniper RADIUS Parameters for a User 7-51
Setting BBSM RADIUS Parameters for a User 7-52
Setting Custom RADIUS Attributes for a User 7-53
User Management 7-54
Listing All Users 7-55
Finding a User 7-55
Disabling a User Account 7-56
Deleting a User Account 7-57
Resetting User Session Quota Counters 7-58
Resetting a User Account after Login Failure 7-59
Saving User Settings 7-60



Downloaded from www.Manualslib.com manuals search engine

CHAPTER 8 **System Configuration: Basic** 8-1

Service Control 8-1

Determining the Status of Cisco Secure ACS Services 8-2

Stopping, Starting, or Restarting Services 8-2

Logging 8-3

Date Format Control 8-3

Setting the Date Format 8-4

Local Password Management 8-5

Configuring Local Password Management 8-7

Cisco Secure ACS Backup 8-9

About Cisco Secure ACS Backup 8-9

Backup File Locations 8-10

Directory Management 8-10

Components Backed Up 8-10

Reports of Cisco Secure ACS Backups 8-11

Backup Options 8-11

Performing a Manual Cisco Secure ACS Backup 8-12

Scheduling Cisco Secure ACS Backups 8-12

Disabling Scheduled Cisco Secure ACS Backups 8-13

Cisco Secure ACS System Restore 8-14

About Cisco Secure ACS System Restore 8-14

Backup Filenames and Locations 8-15

Components Restored 8-16

Reports of Cisco Secure ACS Restorations 8-16

Restoring Cisco Secure ACS from a Backup File 8-16

Cisco Secure ACS Active Service Management 8-17

System Monitoring 8-18

System Monitoring Options 8-18

Setting Up System Monitoring 8-19



Downloaded from www.Manualslib.com manuals search engine

Event Logging 8-20
Setting Up Event Logging 8-20
VoIP Accounting Configuration 8-21
Configuring VoIP Accounting 8-21

CHAPTER 9 **System Configuration: Advanced** 9-1
CiscoSecure Database Replication 9-1
About CiscoSecure Database Replication 9-2
Replication Process 9-4
Replication Frequency 9-7
Important Implementation Considerations 9-7
Database Replication Versus Database Backup 9-10
Database Replication Logging 9-10
Replication Options 9-11
Replication Components Options 9-11
Outbound Replication Options 9-12
Inbound Replication Options 9-15
Implementing Primary and Secondary Replication Setups on Cisco Secure ACSes 9-15
Configuring a Secondary Cisco Secure ACS 9-17
Replicating Immediately 9-19
Scheduling Replication 9-21
Disabling CiscoSecure Database Replication 9-24
Database Replication Event Errors 9-25
RDBMS Synchronization 9-25
About RDBMS Synchronization 9-26
Users 9-27
User Groups 9-27
Network Configuration 9-28
Custom RADIUS Vendors and VSAs 9-28



Downloaded from www.Manualslib.com manuals search engine

RDBMS Synchronization Components 9-29
About CSDBSync 9-29
About the accountActions Table 9-31
Cisco Secure ACS Database Recovery Using the accountActions Table 9-32
Reports and Event (Error) Handling 9-33
Preparing to Use RDBMS Synchronization 9-33
Considerations for Using CSV-Based Synchronization 9-35
Preparing for CSV-Based Synchronization 9-36
Configuring a System Data Source Name for RDBMS Synchronization 9-37
RDBMS Synchronization Options 9-38
RDBMS Setup Options 9-38
Synchronization Scheduling Options 9-39
Synchronization Partners Options 9-39
Performing RDBMS Synchronization Immediately 9-40
Scheduling RDBMS Synchronization 9-41
Disabling Scheduled RDBMS Synchronizations 9-43
IP Pools Server 9-44
About IP Pools Server 9-44
Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges 9-45
Refreshing the AAA Server IP Pools Table 9-47
Adding a New IP Pool 9-47
Editing an IP Pool Definition 9-48
Resetting an IP Pool 9-49
Deleting an IP Pool 9-50
IP Pools Address Recovery 9-51
Enabling IP Pool Address Recovery 9-51

CHAPTER 10 **System Configuration: Authentication and Certificates** 10-1
About Certification and EAP Protocols 10-1
Digital Certificates 10-2



Downloaded from www.Manualslib.com manuals search engine

EAP-TLS Authentication 10-2
About the EAP-TLS Protocol 10-3
EAP-TLS and Cisco Secure ACS 10-4
EAP-TLS Limitations 10-6
Enabling EAP-TLS Authentication 10-7
PEAP Authentication 10-8
About the PEAP Protocol 10-8
PEAP and Cisco Secure ACS 10-9
PEAP and the Unknown User Policy 10-11
Enabling PEAP Authentication 10-12
EAP-FAST Authentication 10-13
About EAP-FAST 10-13
About Master Keys 10-15
About PACs 10-17
Master Key and PAC TTLs 10-21
Replication and EAP-FAST 10-22
Enabling EAP-FAST 10-25
Global Authentication Setup 10-26
Authentication Configuration Options 10-27
Configuring Authentication Options 10-33
Cisco Secure ACS Certificate Setup 10-34
Installing a Cisco Secure ACS Server Certificate 10-35
Adding a Certificate Authority Certificate 10-37
Editing the Certificate Trust List 10-38
Managing Certificate Revocation Lists 10-40
About Certificate Revocation Lists 10-40
Certificate Revocation List Configuration Options 10-41
Adding a Certificate Revocation List Issuer 10-42
Editing a Certificate Revocation List Issuer 10-44
Deleting a Certificate Revocation List Issuer 10-44



Downloaded from www.Manualslib.com manuals search engine

Generating a Certificate Signing Request 10-45
Using Self-Signed Certificates 10-47
About Self-Signed Certificates 10-47
Self-Signed Certificate Configuration Options 10-48
Generating a Self-Signed Certificate 10-49
Updating or Replacing a Cisco Secure ACS Certificate 10-50

CHAPTER 11 **Logs and Reports** 11-1
Logging Formats 11-2
Special Logging Attributes 11-2
NAC Attributes in Logs 11-4
Update Packets in Accounting Logs 11-5
About Cisco Secure ACS Logs and Reports 11-6
Accounting Logs 11-6
Dynamic Administration Reports 11-9
Viewing the Logged-in Users Report 11-10
Deleting Logged-in Users 11-11
Viewing the Disabled Accounts Report 11-12
Cisco Secure ACS System Logs 11-13
Configuring the Administration Audit Log 11-14
Working with CSV Logs 11-15
CSV Log File Names 11-15
CSV Log File Locations 11-16
Enabling or Disabling a CSV Log 11-17
Viewing a CSV Report 11-18
Configuring a CSV Log 11-19
Working with ODBC Logs 11-21
Preparing for ODBC Logging 11-22
Configuring a System Data Source Name for ODBC Logging 11-22



Downloaded from www.Manualslib.com manuals search engine

Configuring an ODBC Log 11-23
Remote Logging 11-26
About Remote Logging 11-26
Implementing Centralized Remote Logging 11-27
Remote Logging Options 11-28
Enabling and Configuring Remote Logging 11-29
Disabling Remote Logging 11-31
Service Logs 11-31
Services Logged 11-32
Configuring Service Logs 11-33

CHAPTER 12 **Administrators and Administrative Policy** 12-1
Administrator Accounts 12-1
About Administrator Accounts 12-2
Administrator Privileges 12-3
Adding an Administrator Account 12-6
Editing an Administrator Account 12-7
Unlocking a Locked Out Administrator Account 12-10
Deleting an Administrator Account 12-11
Access Policy 12-11
Access Policy Options 12-12
Setting Up Access Policy 12-14
Session Policy 12-16
Session Policy Options 12-16
Setting Up Session Policy 12-17
Audit Policy 12-18



Downloaded from www.Manualslib.com manuals search engine

CHAPTER 13 **User Databases** 13-1

CiscoSecure User Database 13-2
About the CiscoSecure User Database 13-2
User Import and Creation 13-3
About External User Databases 13-4
Authenticating with External User Databases 13-5
External User Database Authentication Process 13-6
Windows User Database 13-7
What's Supported with Windows User Databases 13-8
Authentication with Windows User Databases 13-9
Trust Relationships 13-9
Windows Dial-up Networking Clients 13-10
Windows Dial-up Networking Clients with a Domain Field 13-10
Windows Dial-up Networking Clients without a Domain Field 13-11
Usernames and Windows Authentication 13-11
Username Formats and Windows Authentication 13-11
Non-domain-qualified Usernames 13-13
Domain-Qualified Usernames 13-14
UPN Usernames 13-14
EAP and Windows Authentication 13-15
EAP-TLS Domain Stripping 13-16
Machine Authentication 13-16
Machine Access Restrictions 13-19
Microsoft Windows and Machine Authentication 13-20
Enabling Machine Authentication 13-22
User-Changeable Passwords with Windows User Databases 13-25
Preparing Users for Authenticating with Windows 13-26
Windows User Database Configuration Options 13-26
Configuring a Windows External User Database 13-30



Downloaded from www.Manualslib.com manuals search engine

Generic LDAP 13-32
Cisco Secure ACS Authentication Process with a Generic LDAP User Database 13-33
Multiple LDAP Instances 13-33
LDAP Organizational Units and Groups 13-34
Domain Filtering 13-34
LDAP Failover 13-36
Successful Previous Authentication with the Primary LDAP Server 13-36
Unsuccessful Previous Authentication with the Primary LDAP Server 13-37
LDAP Configuration Options 13-37
Configuring a Generic LDAP External User Database 13-43
Novell NDS Database 13-49
About Novell NDS User Databases 13-50
User Contexts 13-51
Novell NDS External User Database Options 13-52
Configuring a Novell NDS External User Database 13-53
ODBC Database 13-55
What is Supported with ODBC User Databases 13-57
Cisco Secure ACS Authentication Process with an ODBC External User Database 13-58
Preparing to Authenticate Users with an ODBC-Compliant Relational Database 13-59
Implementation of Stored Procedures for ODBC Authentication 13-60
Type Definitions 13-61
Microsoft SQL Server and Case-Sensitive Passwords 13-61
Sample Routine for Generating a PAP Authentication SQL Procedure 13-62
Sample Routine for Generating an SQL CHAP Authentication Procedure 13-63
Sample Routine for Generating an EAP-TLS Authentication Procedure 13-64
PAP Authentication Procedure Input 13-64



Downloaded from www.Manualslib.com manuals search engine

PAP Procedure Output 13-65
CHAP/MS-CHAP/ARAP Authentication Procedure Input 13-66
CHAP/MS-CHAP/ARAP Procedure Output 13-66
EAP-TLS Authentication Procedure Input 13-67
EAP-TLS Procedure Output 13-68
Result Codes 13-69
Configuring a System Data Source Name for an ODBC External User Database 13-70
Configuring an ODBC External User Database 13-71
LEAP Proxy RADIUS Server Database 13-75
Configuring a LEAP Proxy RADIUS Server External User Database 13-76
Token Server User Databases 13-78
About Token Servers and Cisco Secure ACS 13-78
Token Servers and ISDN 13-79
RADIUS-Enabled Token Servers 13-79
About RADIUS-Enabled Token Servers 13-80
Token Server RADIUS Authentication Request and Response Contents 13-80
Configuring a RADIUS Token Server External User Database 13-81
RSA SecurID Token Servers 13-84
Configuring an RSA SecurID Token Server External User Database 13-85
Deleting an External User Database Configuration 13-86

CHAPTER 14 **Network Admission Control** 14-1
About Network Admission Control 14-1
NAC AAA Components 14-2
Posture Validation 14-3
Posture Tokens 14-4
Non-Responsive NAC-Client Computers 14-5
Implementing Network Admission Control 14-5



Downloaded from www.Manualslib.com manuals search engine

NAC Databases 14-10
About NAC Databases 14-10
About NAC Credentials and Attributes 14-11
NAC Database Configuration Options 14-12
Policy Selection Options 14-13
Configuring a NAC Database 14-14
NAC Policies 14-16
Local Policies 14-17
About Local Policies 14-18
About Rules, Rule Elements, and Attributes 14-19
Local Policy Configuration Options 14-22
Rule Configuration Options 14-24
Creating a Local Policy 14-25
External Policies 14-28
About External Policies 14-28
External Policy Configuration Options 14-29
Creating an External Policy 14-32
Editing a Policy 14-34
Deleting a Policy 14-36

CHAPTER 15 **Unknown User Policy** 15-1
Known, Unknown, and Discovered Users 15-2
Authentication and Unknown Users 15-4
About Unknown User Authentication 15-4
General Authentication of Unknown Users 15-5
Windows Authentication of Unknown Users 15-6
Domain-Qualified Unknown Windows Users 15-6
Windows Authentication with Domain Qualification 15-7
Multiple User Account Creation 15-8



Downloaded from www.Manualslib.com manuals search engine

Performance of Unknown User Authentication 15-8
Added Authentication Latency 15-9
Authentication Timeout Value on AAA clients 15-9
Posture Validation and the Unknown User Policy 15-10
NAC and the Unknown User Policy 15-10
Posture Validation Use of the Unknown User Policy 15-11
Required Use for Posture Validation 15-12
Authorization of Unknown Users 15-13
Unknown User Policy Options 15-13
Database Search Order 15-14
Configuring the Unknown User Policy 15-16
Disabling Unknown User Authentication 15-17

CHAPTER 16 **User Group Mapping and Specification** 16-1
About User Group Mapping and Specification 16-1
Group Mapping by External User Database 16-2
Creating a Cisco Secure ACS Group Mapping for a Token Server, ODBC Database, or LEAP Proxy RADIUS Server Database 16-3
Group Mapping by Group Set Membership 16-4
Group Mapping Order 16-5
No Access Group for Group Set Mappings 16-5
Default Group Mapping for Windows 16-6
Windows Group Mapping Limitations 16-6
Creating a Cisco Secure ACS Group Mapping for Windows, Novell NDS, or Generic LDAP Groups 16-7
Editing a Windows, Novell NDS, or Generic LDAP Group Set Mapping 16-9
Deleting a Windows, Novell NDS, or Generic LDAP Group Set Mapping 16-10
Deleting a Windows Domain Group Mapping Configuration 16-11
Changing Group Set Mapping Order 16-12



Downloaded from www.Manualslib.com manuals search engine

NAC Group Mapping 16-13
Configuring NAC Group Mapping 16-13
RADIUS-Based Group Specification 16-14

APPENDIX A **Troubleshooting** A-1
Administration Issues A-2
Browser Issues A-4
Cisco IOS Issues A-5
Database Issues A-7
Dial-in Connection Issues A-10
Debug Issues A-14
Proxy Issues A-15
Installation and Upgrade Issues A-16
MaxSessions Issues A-16
Report Issues A-17
Third-Party Server Issues A-19
User Authentication Issues A-20
TACACS+ and RADIUS Attribute Issues A-22

APPENDIX B **TACACS+ Attribute-Value Pairs** B-1
Cisco IOS AV Pair Dictionary B-1
TACACS+ AV Pairs B-2
TACACS+ Accounting AV Pairs B-4

APPENDIX C **RADIUS Attributes** C-1
Cisco IOS Dictionary of RADIUS AV Pairs C-2
Cisco IOS/PIX Dictionary of RADIUS VSAs C-5
About the cisco-av-pair RADUIS Attribute C-7



Downloaded from www.Manualslib.com manuals search engine

Cisco VPN 3000 Concentrator Dictionary of RADIUS VSAs C-9
Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs C-13
Cisco Building Broadband Service Manager Dictionary of RADIUS VSA C-14
IETF Dictionary of RADIUS AV Pairs C-14
Microsoft MPPE Dictionary of RADIUS VSAs C-28
Ascend Dictionary of RADIUS AV Pairs C-31
Nortel Dictionary of RADIUS VSAs C-43
Juniper Dictionary of RADIUS VSAs C-44

APPENDIX D **CSUtil Database Utility** D-1
Location of CSUtil.exe and Related Files D-2
CSUtil.exe Syntax D-2
CSUtil.exe Options D-3
Displaying Command-Line Syntax D-5
Backing Up Cisco Secure ACS with CSUtil.exe D-6
Restoring Cisco Secure ACS with CSUtil.exe D-7
Creating a CiscoSecure User Database D-8
Creating a Cisco Secure ACS Database Dump File D-10
Loading the Cisco Secure ACS Database from a Dump File D-11
Compacting the CiscoSecure User Database D-12
User and AAA Client Import Option D-14
Importing User and AAA Client Information D-15
User and AAA Client Import File Format D-16
About User and AAA Client Import File Format D-17
ONLINE or OFFLINE Statement D-17
ADD Statements D-18
UPDATE Statements D-19
DELETE Statements D-21



Downloaded from www.Manualslib.com manuals search engine

ADD_NAS Statements D-21
DEL_NAS Statements D-23
Import File Example D-24
Exporting User List to a Text File D-24
Exporting Group Information to a Text File D-25
Exporting Registry Information to a Text File D-26
Decoding Error Numbers D-27
Recalculating CRC Values D-28
User-Defined RADIUS Vendors and VSA Sets D-28
About User-Defined RADIUS Vendors and VSA Sets D-29
Adding a Custom RADIUS Vendor and VSA Set D-29
Deleting a Custom RADIUS Vendor and VSA Set D-31
Listing Custom RADIUS Vendors D-32
Exporting Custom RADIUS Vendor and VSA Sets D-33
RADIUS Vendor/VSA Import File D-34
About the RADIUS Vendor/VSA Import File D-34
Vendor and VSA Set Definition D-35
Attribute Definition D-36
Enumeration Definition D-38
Example RADIUS Vendor/VSA Import File D-39
PAC File Generation D-40
PAC File Options and Examples D-41
Generating PAC Files D-43
Posture Validation Attributes D-44
Posture Validation Attribute Definition File D-44
Exporting Posture Validation Attribute Definitions D-48
Importing Posture Validation Attribute Definitions D-49
Deleting a Posture Validation Attribute Definition D-51
Default Posture Validation Attribute Definition File D-52



Downloaded from www.Manualslib.com manuals search engine

APPENDIX E **VPDN Processing** E-1

VPDN Process E-1

APPENDIX F **RDBMS Synchronization Import Definitions** F-1

accountActions Specification F-1

accountActions Format F-2

accountActions Mandatory Fields F-3

accountActions Processing Order F-4

Action Codes F-4

Action Codes for Setting and Deleting Values F-5

Action Codes for Creating and Modifying User Accounts F-7

Action Codes for Initializing and Modifying Access Filters F-14

Action Codes for Modifying TACACS+ and RADIUS Group and User Settings F-19

Action Codes for Modifying Network Configuration F-25

Cisco Secure ACS Attributes and Action Codes F-32

User-Specific Attributes F-32

User-Defined Attributes F-34

Group-Specific Attributes F-35

An Example of accountActions F-36

APPENDIX G **Internal Architecture** G-1

Windows Services G-1

Windows Registry G-2

CSAdmin G-2

CSAuth G-3

CSDBSync G-4

CSLog G-4



Downloaded from www.Manualslib.com manuals search engine

CSMon **G-4**
Monitoring **G-5**
Recording **G-6**
Notification **G-7**
Response **G-7**
CSTacacs and CSRadius **G-8**

INDEX



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

# Preface

This document will help you configure and use Cisco Secure Access Control Server (ACS) and its features and utilities.

## Audience

This guide is for system administrators who use Cisco Secure ACS and who set up and maintain accounts and dial-in network security.

## Organization

This document contains the following chapters and appendixes:

- **Chapter 1, "Overview"**—An overview of Cisco Secure ACS and its features, network diagrams, and system requirements.
- **Chapter 2, "Deployment Considerations"**—A guide to deploying Cisco Secure ACS that includes requirements, options, trade-offs, and suggested sequences.
- **Chapter 3, "Interface Configuration"**—Concepts and procedures regarding how to use the Interface Configuration section of Cisco Secure ACS to configure the HTML interface.
- **Chapter 4, "Network Configuration"**—Concepts and procedures for establishing Cisco Secure ACS network configuration and building a distributed system.



Downloaded from www.Manualslib.com manuals search engine

- **Chapter 5, "Shared Profile Components"**—Concepts and procedures regarding Cisco Secure ACS shared profile components: downloadable IP acls, network access filters, network access restrictions, and device command sets.
- **Chapter 6, "User Group Management"**—Concepts and procedures for establishing and maintaining Cisco Secure ACS user groups.
- **Chapter 7, "User Management"**—Concepts and procedures for establishing and maintaining Cisco Secure ACS user accounts.
- **Chapter 8, "System Configuration: Basic"**—Concepts and procedures regarding the basic features found in the System Configuration section of Cisco Secure ACS.
- **Chapter 9, "System Configuration: Advanced"**—Concepts and procedures regarding RDBMS Synchronization, CiscoSecure Database Replication, and IP pools, found in the System Configuration section of Cisco Secure ACS.
- **Chapter 10, "System Configuration: Authentication and Certificates"**—Concepts and procedures regarding the Global Authentication and ACS Certificate Setup pages, found in the System Configuration section of Cisco Secure ACS.
- **Chapter 11, "Logs and Reports"**—Concepts and procedures regarding Cisco Secure ACS logging and reports.
- **Chapter 12, "Administrators and Administrative Policy"**—Concepts and procedures for establishing and maintaining Cisco Secure ACS administrators.
- **Chapter 13, "User Databases"**—Concepts about user databases and procedures for configuring Cisco Secure ACS to perform user authentication with external user databases.
- **Chapter 14, "Network Admission Control"**—Concepts and procedures for implementing Network Admission Control (NAC) and configuring NAC databases, policies, and rules.
- **Chapter 15, "Unknown User Policy"**—Concepts and procedures about using the Unknown User Policy with posture validation and unknown user authentication.
- **Chapter 16, "User Group Mapping and Specification"**—Concepts and procedures regarding the assignment of groups for users authenticated by an external user database.



Downloaded from www.Manualslib.com manuals search engine

- **Appendix A, "Troubleshooting"**—How to identify and solve certain problems you might have with Cisco Secure ACS.
- **Appendix B, "TACACS+ Attribute-Value Pairs"**—A list of supported TACACS+ AV pairs and accounting AV pairs.
- **Appendix C, "RADIUS Attributes"**—A list of supported RADIUS AV pairs and accounting AV pairs.
- **Appendix D, "CSUtil Database Utility"**—Instructions for using CSUtil.exe, a command line utility you can use to work with the CiscoSecure user database, to import AAA clients and users, to define RADIUS vendors and attributes, and to generate PAC files for EAP-FAST clients.
- **Appendix E, "VPDN Processing"**—An introduction to Virtual Private Dial-up Networks (VPDN), including stripping and tunneling, with instructions for enabling VPDN on Cisco Secure ACS.
- **Appendix F, "RDBMS Synchronization Import Definitions"**—A list of import definitions, for use with the RDBMS Synchronization feature.
- **Appendix G, "Internal Architecture"**—A description of Cisco Secure ACS architectural components.

# Conventions

This document uses the following conventions:

| Item | Convention |
|---|---|
| Commands, keywords, special terminology, and options that should be selected during procedures | **boldface** font |
| Variables for which you supply values and new or important terminology | *italic* font |
| Displayed session and system information, paths and file names | `screen` font |
| Information you enter | **`boldface screen`** font |
| Variables you enter | *italic screen* font |
| Menu items and button names | **boldface** font |
| Indicates menu items to select, in the order you select them. | **Option > Network Preferences** |



Downloaded from www.Manualslib.com manuals search engine

**Tip** Identifies information to help you get the most benefit from your product.

**Note** Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

**Warning** **Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.**

# Product Documentation

**Note** We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

***Table 1 Product Documentation***

| Document Title | Available Formats |
|---|---|
| *Release Notes for Cisco Secure ACS for Windows Server* | • Printed document that was included with the product.<br>• On Cisco.com. |



Downloaded from www.Manualslib.com manuals search engine

*Table 1 Product Documentation (continued)*

| Document Title | Available Formats |
|---|---|
| *Installation Guide for Cisco Secure ACS for Windows Server* | • PDF on the product CD-ROM.<br>• On Cisco.com.<br>• Printed document available by order (part number DOC-7816529=).[1] |
| *User Guide for Cisco Secure ACS for Windows Server* | • PDF on the product CD-ROM.<br>• On Cisco.com.<br>• Printed document available by order (part number DOC-7816530=).[1] |
| *Installation and User Guide for Cisco Secure ACS User-Changeable Passwords* | • PDF on the product CD-ROM.<br>• On Cisco.com. |
| *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS for Windows Server* | • On Cisco.com. |
| *Recommended Resources for the Cisco Secure ACS User* | • On Cisco.com. |
| Online Documentation | In the Cisco Secure ACS HTML interface, click Online Documentation. |
| Online Help | In the Cisco Secure ACS HTML interface, online help appears in the right-hand frame when you are configuring a feature. |

1. See Obtaining Documentation, page xxxv.

# Related Documentation

**Note** We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.



Downloaded from www.Manualslib.com manuals search engine

Table 2 describes a set of white papers about Cisco Secure ACS. All white papers are available on Cisco.com. To view them, go to the following URL:

http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml

***Table 2 Related Documentation***

| Document Title | Description and Available Formats |
|---|---|
| *Building a Scalable TACACS+ Device Management Framework* | This document discusses the key benefits of and how to deploy Cisco Secure ACS Shell Authorization Command sets, which provide the facilities constructing a scalable network device management system using familiar and efficient TCP/IP protocols and utilities supported by Cisco devices. |
| *Catalyst Switching and ACS Deployment Guide* | This document presents planning, design, and implementation practices for deploying Cisco Secure ACS for Windows Server in support of Cisco Catalyst Switch networks. It discusses network topology regarding AAA, user database choices, password protocol choices, access requirements, and capabilities of Cisco Secure ACS. |
| *Cisco Secure ACS for Windows vs. Cisco Secure ACS for UNIX* | This bulletin compares the overall feature sets of Cisco Secure ACS for Windows and CiscoSecure ACS for UNIX. It also examines the advantages and disadvantages of both platforms and discusses issues related to migrating from the UNIX-based product to the Windows version. |
| *Configuring LDAP* | This document outlines deployment concepts for Cisco Secure ACS when authenticating users of a Lightweight Directory Access Protocol (LDAP) directory server, and describes how to use these concepts to configure Cisco Secure ACS. |
| *Deploying Cisco Secure ACS for Windows in a Cisco Aironet Environment* | This paper discusses guidelines for wireless network design and deployment with Cisco Secure ACS. |
| *EAP-TLS Deployment Guide for Wireless LAN Networks* | This document discusses the Extensible Authentication Protocol Transport Layer Security (EAP-TLS) authentication protocol deployment in wireless networks. It introduces the EAP-TLS architecture and then discusses deployment issues. |



Downloaded from www.Manualslib.com manuals search engine

*Table 2 Related Documentation (continued)*

| Document Title | Description and Available Formats |
|---|---|
| *External ODBC Authentication* | This paper presents concepts and configuration issues in deploying Cisco Secure ACS for Windows Server to authenticate users against an external open database connectivity (ODBC) database. This paper also describes configuring, testing, and troubleshooting a relational database management system (RDBMS) with ODBC and Cisco Secure ACS, and provides sample Structured Query Language (SQL) procedures. |
| *Guidelines for Placing ACS in the Network* | This document discusses planning, design, and implementation practices for deploying Cisco Secure ACS for Windows Server in an enterprise network. It discusses network topology, user database choices, access requirements, integration of external databases, and capabilities of Cisco Secure ACS. |
| *Initializing MC Authorization on ACS 3.1* | This application note explains how to initialize Management Center authorization on Cisco Secure ACS. |
| *Securing ACS Running on Microsoft Windows Platforms* | This paper describes how the Cisco Secure ACS can be protected against the vulnerabilities of the Windows 2000 operating system and explains how to improve security on the computer running Cisco Secure ACS. It discusses making the system dedicated to Cisco Secure ACS, removing all unnecessary services, and other measures. It also discusses how to improve administrative security for Cisco Secure ACS through such methods as stronger passwords and controlled administrative access. This paper concludes with considerations of physical security for Cisco Secure ACS and its host. |

# Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.



Downloaded from www.Manualslib.com manuals search engine

# Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

# Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

# Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.



Downloaded from www.Manualslib.com manuals search engine

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

# Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides



Downloaded from www.Manualslib.com manuals search engine

recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

# Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.



Downloaded from www.Manualslib.com manuals search engine

# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine



Downloaded from www.Manualslib.com manuals search engine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html



Downloaded from www.Manualslib.com manuals search engine

# Overview

This chapter provides an overview of Cisco Secure ACS for Windows Server.

This chapter contains the following topics:


- The Cisco Secure ACS Paradigm, page 1-2
- Cisco Secure ACS Specifications, page 1-3
  - System Performance Specifications, page 1-3
  - Cisco Secure ACS Windows Services, page 1-4
- AAA Server Functions and Concepts, page 1-5
  - Cisco Secure ACS and the AAA Client, page 1-6
  - AAA Protocols—TACACS+ and RADIUS, page 1-6
  - Authentication, page 1-8
  - Authorization, page 1-17
  - Accounting, page 1-22
  - Administration, page 1-23
  - Posture Validation, page 1-25
- Cisco Secure ACS HTML Interface, page 1-25
  - About the Cisco Secure ACS HTML Interface, page 1-26
  - HTML Interface Layout, page 1-27
  - Uniform Resource Locator for the HTML Interface, page 1-29
  - Network Environments and Administrative Sessions, page 1-30



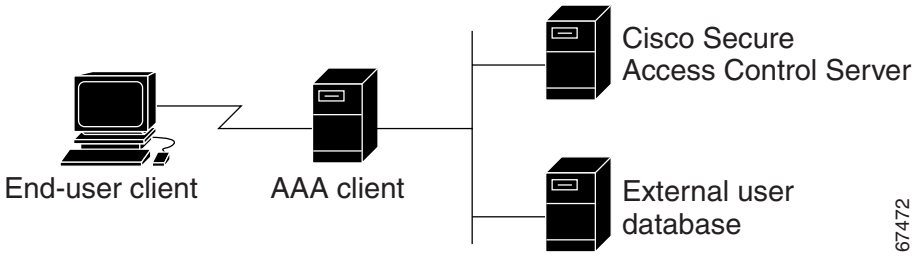

Downloaded from www.Manualslib.com manuals search engine

– Accessing the HTML Interface, page 1-32
– Logging Off the HTML Interface, page 1-33
– Online Help and Online Documentation, page 1-33

# The Cisco Secure ACS Paradigm

Cisco Secure ACS provides authentication, authorization, and accounting (AAA—pronounced "triple A") services to network devices that function as AAA clients, such as a network access server, PIX Firewall, or router. The AAA client in Figure 1-1 represents any such device that provides AAA client functionality and uses one of the AAA protocols supported by Cisco Secure ACS.

***Figure 1-1 A Simple AAA Scenario***




Cisco Secure ACS centralizes access control and accounting, in addition to router and switch access management. With Cisco Secure ACS, network administrators can quickly administer accounts and globally change levels of service offerings for entire groups of users. Although the external user database shown in Figure 1-1 is optional, support for many popular user repository implementations enables companies to put to use the working knowledge gained from and the investment already made in building their corporate user repositories.

Cisco Secure ACS supports Cisco AAA clients such as the Cisco 2509, 2511, 3620, 3640, AS5200 and AS5300, AS5800, the Cisco PIX Firewall, Cisco Aironet Access Point wireless networking devices, Cisco VPN 3000 Concentrators, and Cisco VPN 5000 Concentrators. It also supports third-party devices that can be configured with the Terminal Access Controller Access Control System (TACACS+) or the Remote Access Dial-In User Service (RADIUS) protocol. Cisco Secure ACS treats all such devices as AAA clients. Cisco Secure ACS uses the TACACS+ and RADIUS protocols to provide AAA



Downloaded from www.Manualslib.com manuals search engine

services that ensure a secure environment. For more information about support for TACACS+ and RADIUS in Cisco Secure ACS, see AAA Protocols—TACACS+ and RADIUS, page 1-6.

# Cisco Secure ACS Specifications

**Note** For hardware, operating system, third-party software, and network requirements, see Basic Deployment Requirements for Cisco Secure ACS, page 2-2.

This section contains the following topics:


- System Performance Specifications, page 1-3
- Cisco Secure ACS Windows Services, page 1-4


## System Performance Specifications

The performance capabilities of Cisco Secure ACS are largely dependent upon the Windows server it is installed upon, your network topology and network management, the selection of user databases, and other factors. For example, Cisco Secure ACS can perform many more authentications per second if it is using its internal user database and running on a computer using the fastest processor and network interface card available than it can if it is using several external user databases and running on a computer that complies with the minimum system requirements (see System Requirements, page 2-2).

For more information about the expected performance of Cisco Secure ACS in your network setting, contact your Cisco sales representative. The following items are general answers to common system performance questions. The performance of Cisco Secure ACS in your network depends on your specific environment and AAA requirements.



Downloaded from www.Manualslib.com manuals search engine

- **Maximum users supported by the CiscoSecure user database**—There is no theoretical limit to the number of users the CiscoSecure user database can support. We have successfully tested Cisco Secure ACS with databases in excess of 100,000 users. The practical limit for a single Cisco Secure ACS authenticating against all its databases, internal and external, is 300,000 to 500,000 users. This number increases significantly if the authentication load is spread across a number of replicated Cisco Secure ACSes.
- **Transactions per second**—Authentication and authorization transactions per second is dependent on many factors, most of which are external to Cisco Secure ACS. For example, high network latency in communication with an external user database lowers the transactions per second that Cisco Secure ACS can perform.
- **Maximum number of AAA clients supported**—Cisco Secure ACS can support AAA services for approximately 5000 AAA client configurations. This limitation is primarily a limitation of the Cisco Secure ACS HTML interface. Performance of the HTML interface degrades when Cisco Secure ACS has more than approximately 5000 AAA client configurations. However, a AAA client configuration in Cisco Secure ACS can represent more than one physical network device, provided that the network devices use the same AAA protocol and use the same shared secret. If you make use of this ability, the number of actual AAA clients supported approaches 20,000.

  If your network has several thousand AAA clients, we recommend using multiple Cisco Secure ACSes and assigning no more than 5000 AAA clients to each Cisco Secure ACS. For example, if you have 20,000 AAA clients, you could use four Cisco Secure ACSes and divide the AAA client load among them so that no single Cisco Secure ACS manages more than 5000 AAA client configurations. If you use replication to propagate configuration data among Cisco Secure ACSes, limit replication of AAA client data to Cisco Secure ACSes that serve the same set of AAA clients.

# Cisco Secure ACS Windows Services

Cisco Secure ACS operates as a set of Microsoft Windows services and controls the authentication, authorization, and accounting of users accessing networks.



Downloaded from www.Manualslib.com manuals search engine

When you install Cisco Secure ACS, the installation adds several Windows services. The services provide the core of Cisco Secure ACS functionality. For a full discussion of each service, see Appendix G, "Internal Architecture". The Cisco Secure ACS services on the computer running Cisco Secure ACS include the following:

- **CSAdmin**—Provides the HTML interface for administration of Cisco Secure ACS.
- **CSAuth**—Provides authentication services.
- **CSDBSync**—Provides synchronization of the CiscoSecure user database with an external RDBMS application.
- **CSLog**—Provides logging services, both for accounting and system activity.
- **CSMon**—Provides monitoring, recording, and notification of Cisco Secure ACS performance, and includes automatic response to some scenarios.
- **CSTacacs**—Provides communication between TACACS+ AAA clients and the CSAuth service.
- **CSRadius**—Provides communication between RADIUS AAA clients and the CSAuth service.

Each module can be started and stopped individually from within the Microsoft Service Control Panel or as a group from within the Cisco Secure ACS HTML interface. For information about stopping and starting Cisco Secure ACS services, see Service Control, page 8-1.

# AAA Server Functions and Concepts

Cisco Secure ACS is a AAA server, providing AAA services to network devices that can act as AAA clients.

As a AAA server, Cisco Secure ACS incorporates many technologies to render AAA services to AAA clients. Understanding Cisco Secure ACS requires knowledge of many of these technologies.

This section contains the following topics:

- Cisco Secure ACS and the AAA Client, page 1-6
- AAA Protocols—TACACS+ and RADIUS, page 1-6
- Authentication, page 1-8



Downloaded from www.Manualslib.com manuals search engine

- Authorization, page 1-17
- Accounting, page 1-22
- Administration, page 1-23
- Posture Validation, page 1-25


# Cisco Secure ACS and the AAA Client

A AAA client is software running on a network device that enables the network device to defer authentication, authorization, and logging (accounting) of user sessions to a AAA server. AAA clients must be configured to direct all end-user client access requests to Cisco Secure ACS for authentication of users and authorization of service requests. Using the TACACS+ or RADIUS protocol, the AAA client sends authentication requests to Cisco Secure ACS. Cisco Secure ACS verifies the username and password using the user databases it is configured to query. Cisco Secure ACS returns a success or failure response to the AAA client, which permits or denies user access, based on the response it receives. When the user authenticates successfully, Cisco Secure ACS sends a set of authorization attributes to the AAA client. The AAA client then begins forwarding accounting information to Cisco Secure ACS.

When the user has successfully authenticated, a set of session attributes can be sent to the AAA client to provide additional security and control of privileges, otherwise known as authorization. These attributes might include the IP address pool, access control list, or type of connection (for example, IP, IPX, or Telnet). More recently, networking vendors are expanding the use of the attribute sets returned to cover an increasingly wider aspect of user session provisioning.

# AAA Protocols—TACACS+ and RADIUS

Cisco Secure ACS can use both the TACACS+ and RADIUS AAA protocols. Table 1-1 compares the two protocols.



Downloaded from www.Manualslib.com manuals search engine

*Table 1-1 TACACS+ and RADIUS Protocol Comparison*

| Point of Comparison | TACACS+ | RADIUS |
|---|---|---|
| **Transmission Protocol** | TCP—connection-oriented transport layer protocol, reliable full-duplex data transmission | UDP—connectionless transport layer protocol, datagram exchange without acknowledgments or guaranteed delivery |
| **Ports Used** | 49 | Authentication and Authorization: 1645 and 1812<br>Accounting: 1646 and 1813 |
| **Encryption** | Full packet encryption | Encrypts only passwords up to 16 bytes |
| **AAA Architecture** | Separate control of each service: authentication, authorization, and accounting | Authentication and authorization combined as one service |
| **Intended Purpose** | Device management | User access control |

## TACACS+

Cisco Secure ACS conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.77. For more information, refer to the Cisco IOS software documentation or Cisco.com (http://www.cisco.com).

## RADIUS

Cisco Secure ACS conforms to the RADIUS protocol as defined in draft April 1997 and in the following Requests for Comments (RFCs):

- RFC 2138, Remote Authentication Dial In User Service
- RFC 2139, RADIUS Accounting
- RFC 2865
- RFC 2866
- RFC 2867



Downloaded from www.Manualslib.com manuals search engine

- RFC 2868
- RFC 2869

The ports used for authentication and accounting have changed in RADIUS RFC documents. To support both the older and newer RFCs, Cisco Secure ACS accepts authentication requests on port 1645 and port 1812. For accounting, Cisco Secure ACS accepts accounting packets on port 1646 and 1813.

In addition to support for standard IETF RADIUS attributes, Cisco Secure ACS includes support for RADIUS vendor-specific attributes (VSAs). We have predefined the following RADIUS VSAs in Cisco Secure ACS:

- Cisco IOS/PIX
- Cisco VPN 3000
- Cisco VPN 5000
- Ascend
- Juniper
- Microsoft
- Nortel

Cisco Secure ACS also supports up to 10 RADIUS VSAs that you define. After you define a new RADIUS VSA, you can use it as you would one of the RADIUS VSAs that come predefined in Cisco Secure ACS. In the Network Configuration section of the Cisco Secure ACS HTML interface, you can configure a AAA client to use a user-defined RADIUS VSA as its AAA protocol. In Interface Configuration, you can enable user-level and group-level attributes for user-defined RADIUS VSAs. In User Setup and Group Setup, you can configure the values for enabled attributes of a user-defined RADIUS VSA.

For more information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-28.

# Authentication

Authentication determines user identity and verifies the information. Traditional authentication uses a name and a fixed password. More modern and secure methods use technologies such as CHAP and one-time passwords (OTPs). Cisco Secure ACS supports a variety of these authentication methods.



Downloaded from www.Manualslib.com manuals search engine

There is a fundamental implicit relationship between authentication and authorization. The more authorization privileges granted to a user, the stronger the authentication should be. Cisco Secure ACS supports this relationship by providing various methods of authentication.

This section contains the following topics:


- Authentication Considerations, page 1-9
- Authentication and User Databases, page 1-10
- Authentication Protocol-Database Compatibility, page 1-10
- Passwords, page 1-11
- Other Authentication-Related Features, page 1-16


## Authentication Considerations

Username and password is the most popular, simplest, and least expensive method used for authentication. No special equipment is required. This is a popular method for service providers because of its easy application by the client. The disadvantage is that this information can be told to someone else, guessed, or captured. Simple unencrypted username and password is not considered a strong authentication mechanism but can be sufficient for low authorization or privilege levels such as Internet access.

To reduce the risk of password capturing on the network, use encryption. Client and server access control protocols such as TACACS+ and RADIUS encrypt passwords to prevent them from being captured within a network. However, TACACS+ and RADIUS operate only between the AAA client and the access control server. Before this point in the authentication process, unauthorized persons can obtain clear-text passwords, such as the communication between an end-user client dialing up over a phone line or an ISDN line terminating at a network access server, or over a Telnet session between an end-user client and the hosting device.

Network administrators who offer increased levels of security services, and corporations that want to lessen the chance of intruder access resulting from password capturing, can use an OTP. Cisco Secure ACS supports several types of OTP solutions, including PAP for Point-to-Point Protocol (PPP) remote-node login. Token cards are considered one of the strongest OTP authentication mechanisms.



Downloaded from www.Manualslib.com manuals search engine

## Authentication and User Databases

Cisco Secure ACS supports a variety of user databases. It supports the CiscoSecure user database and several external user databases, including the following:

- Windows User Database
- Generic LDAP
- Novell NetWare Directory Services (NDS)
- Open Database Connectivity (ODBC)-compliant relational databases
- RSA SecurID token server
- RADIUS-compliant token servers

**Note** For more information about token server support, see Token Server User Databases, page 13-78

## Authentication Protocol-Database Compatibility

The various password protocols supported by Cisco Secure ACS for authentication are supported unevenly by the various databases supported by Cisco Secure ACS. For more information about the password protocols supported by Cisco Secure ACS, see Passwords, page 1-11.

Table 1-2 specifies non-EAP authentication protocol support.

*Table 1-2 Non-EAP Authentication Protocol and User Database Compatibility*

| Database | ASCII/PAP | CHAP | ARAP | MS-CHAP v.1 | MS-CHAP v.2 |
|---|---|---|---|---|---|
| Cisco Secure ACS | Yes | Yes | Yes | Yes | Yes |
| Windows SAM | Yes | No | No | Yes | Yes |
| Windows AD | Yes | No | No | Yes | Yes |
| LDAP | Yes | No | No | No | No |
| Novell NDS | Yes | No | No | No | No |
| ODBC | Yes | Yes | Yes | Yes | Yes |



Downloaded from www.Manualslib.com manuals search engine

*Table 1-2 Non-EAP Authentication Protocol and User Database Compatibility (continued)*

| Database | ASCII/PAP | CHAP | ARAP | MS-CHAP v.1 | MS-CHAP v.2 |
|---|---|---|---|---|---|
| LEAP Proxy RADIUS Server | Yes | No | No | Yes | Yes |
| All Token Servers | Yes | No | No | No | No |

Table 1-3 specifies EAP authentication protocol support.

*Table 1-3 EAP Authentication Protocol and User Database Compatibility*

| Database | LEAP | EAP-MD5 | EAP-TLS | PEAP (EAP-GTC) | PEAP (EAP-MS CHAPv2) | EAP-FAST Phase Zero | EAP-FAST Phase Two |
|---|---|---|---|---|---|---|---|
| Cisco Secure ACS | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Windows SAM | Yes | No | No | Yes | Yes | Yes | Yes |
| Windows AD | Yes | No | Yes | Yes | Yes | Yes | Yes |
| LDAP | No | No | Yes | Yes | No | No | Yes |
| Novell NDS | No | No | No | Yes | No | No | Yes |
| ODBC | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| LEAP Proxy RADIUS Server | Yes | No | No | Yes | Yes | Yes | Yes |
| All Token Servers | No | No | No | Yes | No | No | No |

## Passwords

Cisco Secure ACS supports many common password protocols:

- ASCII/PAP
- CHAP
- MS-CHAP
- LEAP
- EAP-MD5
- EAP-TLS



Downloaded from www.Manualslib.com manuals search engine

- PEAP(EAP-GTC)
- PEAP(EAP-MSCHAPv2)
- EAP-FAST
- ARAP

Passwords can be processed using these password authentication protocols based on the version and type of security control protocol used (for example, RADIUS or TACACS+) and the configuration of the AAA client and end-user client. The following sections outline the different conditions and functions of password handling.

In the case of token servers, Cisco Secure ACS acts as a client to the token server, using either its proprietary API or its RADIUS interface, depending on the token server. For more information, see About Token Servers and Cisco Secure ACS, page 13-78.

Different levels of security can be concurrently used with Cisco Secure ACS for different requirements. The basic user-to-network security level is PAP. Although it represents the unencrypted security, PAP does offer convenience and simplicity for the client. PAP allows authentication against the Windows database. With this configuration, users need to log in only once. CHAP allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client. You can use CHAP with the CiscoSecure user database. ARAP support is included to support Apple clients.

## Comparing PAP, CHAP, and ARAP

PAP, CHAP, and ARAP are authentication protocols used to encrypt passwords. However, each protocol provides a different level of security.

- **PAP**—Uses clear-text passwords (that is, unencrypted passwords) and is the least sophisticated authentication protocol. If you are using the Windows user database to authenticate users, you must use PAP password encryption or MS-CHAP.
- **CHAP**—Uses a challenge-response mechanism with one-way encryption on the response. CHAP enables Cisco Secure ACS to negotiate downward from the most secure to the least secure encryption mechanism, and it protects passwords transmitted in the process. CHAP passwords are reusable. If you are using the CiscoSecure user database for authentication, you can use either PAP or CHAP. CHAP does not work with the Windows user database.



Downloaded from www.Manualslib.com manuals search engine

- **ARAP**—Uses a two-way challenge-response mechanism. The AAA client challenges the end-user client to authenticate itself, and the end-user client challenges the AAA client to authenticate itself.

## MS-CHAP

Cisco Secure ACS supports Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) for user authentication. Differences between MS-CHAP and standard CHAP are the following:

- The MS-CHAP Response packet is in a format compatible with Microsoft Windows and LAN Manager 2.x. The MS-CHAP format does not require the authenticator to store a clear-text or reversibly encrypted password.
- MS-CHAP provides an authentication-retry mechanism controlled by the authenticator.
- MS-CHAP provides additional failure codes in the Failure packet Message field.

For more information on MS-CHAP, refer to RFC draft-ietf-pppext-mschap-00.txt, RADIUS Attributes for MS-CHAP Support.

## EAP Support

The Extensible Authentication Protocol (EAP), based on IETF 802.1x, is an end-to-end framework that allows the creation of authentication types without changing AAA client configurations. For more information about EAP, go to PPP Extensible Authentication Protocol (EAP) RFC 2284.

Cisco Secure ACS supports the following varieties of EAP:

- **EAP-MD5**—An EAP protocol that does not support mutual authentication.
- **EAP-TLS**—EAP incorporating Transport Layer Security. For more information, see EAP-TLS Deployment Guide for Wireless LAN Networks and EAP-TLS Authentication, page 10-2.
- **LEAP**—An EAP protocol used by Cisco Aironet wireless equipment; it supports mutual authentication.
- **PEAP**—Protected EAP, which is implemented with EAP-Generic Token Card (GTC) and EAP-MSCHAPv2 protocols. For more information, see PEAP Authentication, page 10-8.



Downloaded from www.Manualslib.com manuals search engine

- **EAP-FAST**—EAP Flexible Authentication via Secured Tunnel (EAP-FAST), a faster means of encrypting EAP authentication, supports EAP-GTC authentication. For more information, see EAP-FAST Authentication, page 10-13.

The architecture of Cisco Secure ACS is extensible with regard to EAP; additional varieties of EAP will be supported as those protocols mature.

## Basic Password Configurations

There are several basic password configurations:

**Note** These configurations are all classed as inbound authentication.

- **Single password for ASCII/PAP/CHAP/MS-CHAP/ARAP**—This is the most convenient method for both the administrator when setting up accounts and the user when obtaining authentication. However, because the CHAP password is the same as the PAP password, and the PAP password is transmitted in clear text during an ASCII/PAP login, there is the chance that the CHAP password can be compromised.
- **Separate passwords for ASCII/PAP and CHAP/MS-CHAP/ARAP**—For a higher level of security, users can be given two separate passwords. If the ASCII/PAP password is compromised, the CHAP/ARAP password can remain secure.
- **External user database authentication**—For authentication by an external user database, the user does not need a password stored in the CiscoSecure user database. Instead, Cisco Secure ACS records which external user database it should query to authenticate the user.

## Advanced Password Configurations

Cisco Secure ACS supports the following advanced password configurations:

- **Inbound passwords**—Passwords used by most Cisco Secure ACS users. These are supported by both the TACACS+ and RADIUS protocols. They are held internally to the CiscoSecure user database and are not usually given up to an external source if an outbound password has been configured.



Downloaded from www.Manualslib.com manuals search engine

- **Outbound passwords**—The TACACS+ protocol supports outbound passwords that can be used, for example, when a AAA client has to be authenticated by another AAA client and end-user client. Passwords from the CiscoSecure user database are then sent back to the second AAA client and end-user client.
- **Token caching**—When token caching is enabled, ISDN users can connect (for a limited time) a second B Channel using the same OTP entered during original authentication. For greater security, the B-Channel authentication request from the AAA client should include the OTP in the username value (for example, Fred*password*) while the password value contains an ASCII/PAP/ARAP password. The TACACS+ and RADIUS servers then verify that the token is still cached and validate the incoming password against either the single ASCII/PAP/ARAP or separate CHAP/ARAP password, depending on the configuration the user employs.

  The TACACS+ SENDAUTH feature enables a AAA client to authenticate itself to another AAA client or an end-user client via outbound authentication. The outbound authentication can be PAP, CHAP, or ARAP. With outbound authentication, the Cisco Secure ACS password is given out. By default, ASCII/PAP or CHAP/ARAP password is used, depending on how this has been configured; however, we recommend that the separate SENDAUTH password be configured for the user so that Cisco Secure ACS inbound passwords are never compromised.

If you want to use outbound passwords and maintain the highest level of security, we recommend that you configure users in the CiscoSecure user database with an outbound password that is different from the inbound password.

## Password Aging

With Cisco Secure ACS you can choose whether and how you want to employ password aging. Control for password aging may reside either in the CiscoSecure user database, or in a Windows user database. Each password aging mechanism differs as to requirements and setting configurations.

The password aging feature controlled by the CiscoSecure user database enables you force users to change their passwords under any of the following conditions:

- After a specified number of days.
- After a specified number of logins.
- The first time a new user logs in.



Downloaded from www.Manualslib.com manuals search engine

For information on the requirements and configuration of the password aging feature controlled by the CiscoSecure user database, see Enabling Password Aging for the CiscoSecure User Database, page 6-21.

The Windows-based password aging feature enables you to control the following password aging parameters:

- Maximum password age in days.
- Minimum password age in days.

The methods and functionality of Windows password aging differ according to which Windows operating system you use and whether you employ Active Directory (AD) or Security Accounts Manager (SAM). For information on the requirements and configuration of the Windows-based password aging feature, see Enabling Password Aging for Users in Windows Databases, page 6-26.

### User-Changeable Passwords

With Cisco Secure ACS, you can install a separate program that enables users to change their passwords by using a web-based utility. For more information about installing user-changeable passwords, see the *Installation and User Guide for Cisco Secure ACS User-Changeable Passwords*.

## Other Authentication-Related Features

In addition to the authentication-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Authentication of unknown users with external user databases (see About Unknown User Authentication, page 15-4).
- Authentication of computers running Microsoft Windows (see Machine Authentication, page 13-16).
- Support for the Microsoft Windows Callback feature (see Setting User Callback Option, page 7-9).
- Ability to configure user accounts, including passwords, using an external data source (see About RDBMS Synchronization, page 9-26).
- Ability for external users to authenticate via an enable password (see Setting TACACS+ Enable Password Options for a User, page 7-35).
- Proxy of authentication requests to other AAA servers (see Proxy in Distributed Systems, page 4-4).



Downloaded from www.Manualslib.com manuals search engine

- Configurable character string stripping from proxied authentication requests (see Stripping, page 4-6).
- Self-signed server certificates (see Using Self-Signed Certificates, page 10-47).
- Certificate revocation list checking during EAP-TLS authentication (see Managing Certificate Revocation Lists, page 10-40).

# Authorization

Authorization determines what a user is allowed to do. Cisco Secure ACS can send user profile policies to a AAA client to determine the network services the user can access. You can configure authorization to give different users and groups different levels of service. For example, standard dial-up users might not have the same access privileges as premium customers and users. You can also differentiate by levels of security, access times, and services.

The Cisco Secure ACS access restrictions feature enables you to permit or deny logins based on time-of-day and day-of-week. For example, you could create a group for temporary accounts that can be disabled on specified dates. This would make it possible for a service provider to offer a 30-day free trial. The same authorization could be used to create a temporary account for a consultant with login permission limited to Monday through Friday, 9 A.M. to 5 P.M.

You can restrict users to a service or combination of services such as PPP, AppleTalk Remote Access (ARA), Serial Line Internet Protocol (SLIP), or EXEC. After a service is selected, you can restrict Layer 2 and Layer 3 protocols, such as IP and IPX, and you can apply individual access lists. Access lists on a per-user or per-group basis can restrict users from reaching parts of the network where critical information is stored or prevent them from using certain services such as File Transfer Protocol (FTP) or Simple Network Management Protocol (SNMP).

One fast-growing service being offered by service providers and adopted by corporations is a service authorization for Virtual Private Dial-Up Networks (VPDNs). Cisco Secure ACS can provide information to the network device for a specific user to configure a secure tunnel through a public network such as the Internet. The information can be for the access server (such as the home gateway for that user) or for the home gateway router to validate the user at the customer premises. In either case, Cisco Secure ACS can be used for each end of the VPDN.



Downloaded from www.Manualslib.com manuals search engine

This section contains the following topics:


- MaxSessions Issues, page A-16
- Dynamic Usage Quotas, page 1-18
- Shared Profile Components, page 1-19
- Support for Cisco Device-Management Applications, page 1-19
- Other Authorization-Related Features, page 1-21


## Max Sessions

Max Sessions is a useful feature for organizations that need to limit the number of concurrent sessions available to either a user or a group:

- **User Max Sessions**—For example, an Internet service provider can limit each account holder to a single session.
- **Group Max Sessions**—For example, an enterprise administrator can allow the remote access infrastructure to be shared equally among several departments and limit the maximum number of concurrent sessions for all users in any one department.

In addition to enabling simple User and Group Max Sessions control, Cisco Secure ACS enables the administrator to specify a Group Max Sessions value and a group-based User Max Sessions value; that is, a User Max Sessions value based on the group membership of the user. For example, an administrator can allocate a Group Max Sessions value of 50 to the group "Sales" and also limit each member of the "Sales" group to 5 sessions each. This way no single member of a group account would be able to use more than 5 sessions at any one time, but the group could still have up to 50 active sessions.

For more information about the Max Sessions feature, see Setting Max Sessions for a User Group, page 6-12 and Setting Max Sessions Options for a User, page 7-16.

## Dynamic Usage Quotas

Cisco Secure ACS enables you to define network usage quotas for users. Using quotas, you can limit the network access of each user in a group or of individual users. You define quotas by duration of sessions or the total number of sessions.



Downloaded from www.Manualslib.com manuals search engine

Quotas can be either absolute or based on daily, weekly, or monthly periods. To grant access to users who have exceeded their quotas, you can reset session quota counters as needed.

To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated only when the user logs off and the accounting stop packet is received from the AAA client. If the AAA client through which the user is accessing your network fails, the session information is not updated. In the case of multiple sessions, such as with ISDN, the quota would not be updated until all sessions terminate, which means that a second channel will be accepted even if the first channel has exhausted the quota allocated to the user.

For more information about usage quotas, see Setting Usage Quotas for a User Group, page 6-14 and Setting User Usage Quotas Options, page 7-18.

## Shared Profile Components

Cisco Secure ACS provides a means for specifying authorization profile components that you can apply to multiple user groups and users. For example, you may have multiple user groups that have identical network access restrictions. Rather than configuring the network access restrictions several times, once per group, you can configure a network access restriction set in the Shared Profile Components section of the HTML interface, and then configure each group to use the network access restriction set you created.

For information about the types of shared profile components supported by Cisco Secure ACS, see About Shared Profile Components, page 5-1.

## Support for Cisco Device-Management Applications

Cisco Secure ACS supports Cisco device-management applications, such as, by providing command authorization for network users who are using the management application to configure managed network devices. Support for command authorization for management application users is accomplished by using unique command authorization set types for each management application configured to use Cisco Secure ACS for authorization.

Cisco Secure ACS uses TACACS+ to communicate with management applications. For a management application to communicate with Cisco Secure ACS, the management application must be configured in Cisco Secure ACS as a



Downloaded from www.Manualslib.com manuals search engine

AAA client that uses TACACS+. Also, you must provide the device-management application with a valid administrator name and password. When a management application initially communicates with Cisco Secure ACS, these requirements ensure the validity of the communication. For information about configuring a AAA client, see AAA Client Configuration, page 4-11. For information about administrator accounts, see Administrator Accounts, page 12-1.

Additionally, the administrator used by the management application must have the Create New Device Command Set Type privilege enabled. When a management application initially communicates with Cisco Secure ACS, it dictates to Cisco Secure ACS the creation of a device command set type, which appears in the Shared Profile Components section of the HTML interface. It also dictates a custom service to be authorized by TACACS+. The custom service appears on the TACACS+ (Cisco IOS) page in the Interface Configuration section of the HTML interface. For information about enabling TACACS+ services, see Protocol Configuration Options for TACACS+, page 3-7. For information about device command-authorization sets for management applications, see Command Authorization Sets, page 5-25.

After the management application has dictated the custom TACACS+ service and device command-authorization set type to Cisco Secure ACS, you can configure command-authorization sets for each role supported by the management application and apply those sets to user groups that contain network administrators or to individual users who are network administrators. For information about configuring a command-authorization set, see Adding a Command Authorization Set, page 5-31. For information about applying a shared device command-authorization set to a user group, see Configuring Device-Management Command Authorization for a User Group, page 6-37. For information about applying a shared device command-authorization set to a user, see Configuring Device-Management Command Authorization for a User, page 7-30.



Downloaded from www.Manualslib.com manuals search engine

## Other Authorization-Related Features

In addition to the authorization-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Group administration of users, with support for 500 groups (see Chapter 6, "User Group Management").
- Ability to map a user from an external user database to a specific Cisco Secure ACS group (see Chapter 16, "User Group Mapping and Specification").
- Ability to disable an account after a number of failed attempts, specified by the administrator (see Setting Options for User Account Disablement, page 7-20).
- Ability to disable an account on a specific date (see Setting Options for User Account Disablement, page 7-20).
- Ability to disable groups of users (see Group Disablement, page 6-4).
- Ability to restrict time-of-day and day-of-week access (see Setting Default Time-of-Day Access for a User Group, page 6-5).
- Network access restrictions (NARs) based on remote address caller line identification (CLID) and dialed number identification service (DNIS) (see Setting Network Access Restrictions for a User Group, page 6-8).
- Downloadable ACLs for users or groups, enabling centralized, modular ACL management (see Downloadable IP ACLs, page 5-7).
- Network access filters, enabling you to apply different downloadable ACLs and NARs based upon a user's point of entry into your network (see Network Access Filters, page 5-2).
- IP pools for IP address assignment of end-user client hosts (see Setting IP Address Assignment Method for a User Group, page 6-28).
- Per-user and per-group TACACS+ or RADIUS attributes (see Advanced Options, page 3-4).
- Support for Voice-over-IP (VoIP), including configurable logging of accounting data (see Enabling VoIP Support for a User Group, page 6-4).



Downloaded from www.Manualslib.com manuals search engine

# Accounting

AAA clients use the accounting functions provided by the RADIUS and TACACS+ protocols to communicate relevant data for each user session to the AAA server for recording. Cisco Secure ACS writes accounting records to a comma-separated value (CSV) log file or ODBC database, depending upon your configuration. You can easily import these logs into popular database and spreadsheet applications for billing, security audits, and report generation. You can also use a third-party reporting tool to manage accounting data. For example, aaa-reports! by Extraxi supports Cisco Secure ACS (http://www.extraxi.com).

Among the types of accounting logs you can generate are the following:

- **TACACS+ Accounting**—Lists when sessions start and stop; records AAA client messages with username; provides caller line identification information; records the duration of each session.
- **RADIUS Accounting**—Lists when sessions stop and start; records AAA client messages with username; provides caller line identification information; records the duration of each session.
- **Administrative Accounting**—Lists commands entered on a network device with TACACS+ command authorization enabled.

For more information about Cisco Secure ACS logging capabilities, see Chapter 11, "Logs and Reports".

## Other Accounting-Related Features

In addition to the accounting-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Centralized logging, allowing several Cisco Secure ACS for Windows Server installations to forward their accounting data to a remote Cisco Secure ACS (see Remote Logging, page 11-26).
- Configurable supplementary user ID fields for capturing additional information in logs (see User Data Configuration Options, page 3-3).
- Configurable logs, allowing you to capture as much information as needed (see Accounting Logs, page 11-6).



Downloaded from www.Manualslib.com manuals search engine

# Administration

To configure, maintain, and protect its AAA functionality, Cisco Secure ACS provides a flexible administration scheme. You can perform nearly all administration of Cisco Secure ACS through its HTML interface. For more information about the HTML interface, including steps for accessing the HTML interface, see Cisco Secure ACS HTML Interface, page 1-25.

This section contains the following topics:


- HTTP Port Allocation for Administrative Sessions, page 1-23
- Network Device Groups, page 1-24
- Other Administration-Related Features, page 1-24


## HTTP Port Allocation for Administrative Sessions

The HTTP port allocation feature allows you to configure the range of TCP ports used by Cisco Secure ACS for administrative HTTP sessions. Narrowing this range with the HTTP port allocation feature reduces the risk of unauthorized access to your network by a port open for administrative sessions.

We do not recommend that you administer Cisco Secure ACS through a firewall. Doing so requires that you configure the firewall to permit HTTP traffic over the range of HTTP administrative session ports that Cisco Secure ACS uses. While narrowing this range reduces the risk of unauthorized access, a greater risk of attack remains if you allow administration of Cisco Secure ACS from outside a firewall. A firewall configured to permit HTTP traffic over the Cisco Secure ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port a web browser must address to initiate an administrative session.

**Note** A broad HTTP port range could create a security risk. To prevent accidental discovery of an active administrative port by unauthorized users, keep the HTTP port range as narrow as possible. Cisco Secure ACS tracks the IP address associated with each administrative session. An unauthorized user would have to impersonate, or “spoof”, the IP address of the legitimate remote host to make use of the active administrative session HTTP port.



Downloaded from www.Manualslib.com manuals search engine

For information about configuring the HTTP port allocation feature, see Access Policy, page 12-11.

## Network Device Groups

With a network device group (NDG), you can view and administer a collection of AAA clients and AAA servers as a single logical group. To simplify administration, you can assign each group a convenient name that can be used to refer to all devices within that group. This creates two levels of network devices within Cisco Secure ACS—discrete devices such as an individual router, access server, AAA server, or PIX Firewall, and NDGs, which are named collections of AAA clients and AAA servers.

A network device can belong to only one NDG at a time.

Using NDGs enables an organization with a large number of AAA clients spread across a large geographical area to logically organize its environment within Cisco Secure ACS to reflect the physical setup. For example, all routers in Europe could belong to a group named Europe; all routers in the United States could belong to a US group; and so on. This would be especially convenient if the AAA clients in each region were administered along the same divisions. Alternatively, the environment could be organized by some other attribute such as divisions, departments, business functions, and so on.

You can assign a group of users to an NDG. For more information on NDGs, see Network Device Group Configuration, page 4-28.

## Other Administration-Related Features

In addition to the administration-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Ability to define different privileges per administrator (see Administrator Accounts, page 12-1).
- Ability to log administrator activities (see Cisco Secure ACS System Logs, page 11-13).
- Ability to view a list of logged-in users (see Dynamic Administration Reports, page 11-9).



Downloaded from www.Manualslib.com manuals search engine

- CSMonitor service, providing monitoring, notification, logging, and limited automated failure response (see Cisco Secure ACS Active Service Management, page 8-17).
- Ability to automate configuration of users, groups, network devices, and custom RADIUS VSAs (see RDBMS Synchronization, page 9-25).
- Replication of CiscoSecure user database components to other Cisco Secure ACSes (see CiscoSecure Database Replication, page 9-1).
- Scheduled and on-demand Cisco Secure ACS system backups (see Cisco Secure ACS Backup, page 8-9).
- Ability to restore Cisco Secure ACS configuration, user accounts, and group profiles from a backup file (see Cisco Secure ACS System Restore, page 8-14).

## Posture Validation

Cisco Secure ACS supports Network Admission Control (NAC) by providing posture validation services to NAC-compliant AAA clients and the NAC-client computers seeking network access using those AAA clients. NAC provides a powerful means to defend your network. The data with which you can configure Cisco Secure ACS to evaluate posture validation requests can include operating system patch level and anti-virus DAT file versions and dates.

Instead of establishing identity, posture validation determines the state of the NAC-client computer using data sent to Cisco Secure ACS by the NAC client. Cisco Secure ACS uses the result of evaluating the state of the computer to determine whether network access is to be granted from the computer and to determine the degree of that access.

For more information, see Chapter 14, “Network Admission Control”.

# Cisco Secure ACS HTML Interface

This section discusses the Cisco Secure ACS HTML interface and provides procedures for using it.



Downloaded from www.Manualslib.com manuals search engine

This section contains the following topics:


- About the Cisco Secure ACS HTML Interface, page 1-26
- HTML Interface Layout, page 1-27
- Uniform Resource Locator for the HTML Interface, page 1-29
- Network Environments and Administrative Sessions, page 1-30
- Accessing the HTML Interface, page 1-32
- Logging Off the HTML Interface, page 1-33
- Online Help and Online Documentation, page 1-33


# About the Cisco Secure ACS HTML Interface

After installing Cisco Secure ACS, you configure and administer it through the HTML interface. The HTML interface enables you to easily modify Cisco Secure ACS configuration from any connection on your LAN or WAN.

The Cisco Secure ACS HTML interface is designed to be viewed using a web browser. The design primarily uses HTML, along with some Java functions, to enhance ease of use. This design keeps the interface responsive and straightforward. The inclusion of Java requires that the browser used for administrative sessions supports Java. For a list of supported browsers, see the Release Notes. The most recent revision to the Release Notes is posted on Cisco.com (http://www.cisco.com).

The HTML interface not only makes viewing and editing user and group information possible, it also enables you to restart services, add remote administrators, change AAA client information, back up the system, view reports from anywhere on the network, and more. The reports track connection activity, show which users are logged in, list failed authentication and authorization attempts, and show administrators' recent tasks.

## HTML Interface Security

Accessing the HTML interface requires a valid administrator name and password. The Cisco Secure ACS Login page encrypts the administrator credentials before sending them to Cisco Secure ACS.



Downloaded from www.Manualslib.com manuals search engine

Administrative sessions timeout after a configurable length of idle time. Regardless, we recommend that you log out of the HTML interface after each session. For information about logging out of Cisco Secure ACS, see Logging Off the HTML Interface, page 1-33. For information about configuring the idle timeout feature, see Access Policy, page 12-11.

You can enable secure socket layer (SSL) for administrative sessions. This ensures that all communication between the web browser and Cisco Secure ACS is encrypted. Your browser must support SSL. You can enable this feature on the Access Policy Setup page in the Administration Control section. For more information about enabling SSL for HTML interface security, see Access Policy, page 12-11.

# HTML Interface Layout

The HTML interface has three vertical partitions, known as frames:

- **Navigation Bar**—The gray frame on the left of the browser window, the navigation bar contains the task buttons. Each button changes the configuration area (see below) to a unique section of the Cisco Secure ACS application, such as the User Setup section or the Interface Configuration section. This frame does not change; it always contains the following buttons:
  - **User Setup**—Add and edit user profiles. For more information about the User Setup section, see Chapter 7, "User Management".
  - **Group Setup**—Configure network services and protocols for groups of users. For more information about the Group Setup section, see Chapter 6, "User Group Management".
  - **Shared Profile Components**—Add and edit network access restriction and command authorization sets, to be applied to users and groups. For more information about the Shared Profile Components section, see Chapter 5, "Shared Profile Components".
  - **Network Configuration**—Add and edit network access devices and configure distributed systems. For more information about the Network Configuration section, see Chapter 4, "Network Configuration".
  - **System Configuration**—Configure system-level features. Four chapters address this large section of the HTML interface. For information about fundamental features such as backup scheduling and service controls, see Chapter 8, "System Configuration: Basic". For information about



Downloaded from www.Manualslib.com manuals search engine

advanced features such as database replication, see Chapter 9, "System Configuration: Advanced". For information about configuring authentication protocols and certificate-related features, see Chapter 10, "System Configuration: Authentication and Certificates". For information about configuring logs and reports, see Chapter 11, "Logs and Reports".

- **Interface Configuration**—Display or hide product features and options to be configured. For more information about the Interface Configuration section, Chapter 3, "Interface Configuration".
- **Administration Control**—Define and configure access policies. For more information about the Administration Control section, Chapter 12, "Administrators and Administrative Policy".
- **External User Databases**—Configure databases, the Unknown User Policy, and user group mapping. For information about configuring databases, see Chapter 13, "User Databases". For information about the Unknown User Policy, see Chapter 15, "Unknown User Policy". For information about user group mapping, see Chapter 16, "User Group Mapping and Specification".
- **Reports and Activity**—Display accounting and logging information. For information about viewing reports, see Chapter 11, "Logs and Reports".
- **Online Documentation**—View the user guide. For information about using the online documentation, see Online Help and Online Documentation, page 1-33.

- **Configuration Area**—The frame in the middle of the browser window, the configuration area displays web pages that belong to one of the sections represented by the buttons in the navigation bar. The configuration area is where you add, edit, or delete information. For example, you configure user information in this frame on the User Setup Edit page.

**Note** Most pages have a Submit button at the bottom. Click Submit to confirm your changes. If you do not click Submit, changes are not saved.

- **Display Area**—The frame on the right of the browser window, the display area shows one of the following options:



Downloaded from www.Manualslib.com manuals search engine

- **Online Help**—Displays basic help about the page currently shown in the configuration area. This help does not offer in-depth information, rather it gives some basic information about what can be accomplished in the middle frame. For more information about online help, see Using Online Help, page 1-34.
- **Reports or Lists**—Displays lists or reports, including accounting reports. For example, in User Setup you can show all usernames that start with a specific letter. The list of usernames beginning with a specified letter is displayed in this section. The usernames are hyperlinks to the specific user configuration, so clicking the name enables you to edit that user.
- **System Messages**—Displays messages after you click Submit if you have typed in incorrect or incomplete data. For example, if the information you entered in the Password box does not match the information in the Confirm Password box in the User Setup section, Cisco Secure ACS displays an error message here. The incorrect information remains in the configuration area so that you can retype and resubmit the information correctly.

# Uniform Resource Locator for the HTML Interface

You can access the Cisco Secure ACS HTML interface by using one of the following uniform resource locators (URLs):

- http://*IP address*:2002
- http://*hostname*:2002

where *IP address* is the dotted decimal IP address of the computer running Cisco Secure ACS and *hostname* is the hostname of the computer running Cisco Secure ACS. If you use the hostname, DNS must be functioning properly on your network or the hostname must be listed in the local hosts file of the computer running the browser.

If Cisco Secure ACS is configured to use SSL to protect administrative sessions, you can also access the HTML interface by specifying the HTTPS protocol in the URLs:

- https://*IP address*:2002
- https://*hostname*:2002



Downloaded from www.Manualslib.com manuals search engine

If SSL is enabled and you do not specify HTTPS, Cisco Secure ACS redirects the initial request to HTTPS for you. Using SSL to access the login page protects administrator credentials. For more information about enabling SSL to protect administrative sessions, see Access Policy, page 12-11.

From the computer running Cisco Secure ACS, you can also use the following URLs:

- http://127.0.0.1:2002
- http://*hostname*:2002

where *hostname* is the hostname of the computer running Cisco Secure ACS. If SSL is enabled, you can specify the HTTP protocol in the URLs:

- https://127.0.0.1:2002
- https://*hostname*:2002

# Network Environments and Administrative Sessions

We recommend that administrative sessions take place without the use of an HTTP proxy server, without a firewall between the browser and Cisco Secure ACS, and without a NAT gateway between the browser and Cisco Secure ACS. Because these limitations are not always practical, this section discusses how various network environmental issues affect administrative sessions.

This section contains the following topics:

- Administrative Sessions and HTTP Proxy, page 1-30
- Administrative Sessions through Firewalls, page 1-31
- Administrative Sessions through a NAT Gateway, page 1-31

## Administrative Sessions and HTTP Proxy

Cisco Secure ACS does not support HTTP proxy for administrative sessions. If the browser used for an administrative session is configured to use a proxy server, Cisco Secure ACS sees the administrative session originating from the IP address of the proxy server rather than from the actual address of the computer. Administrative session tracking assumes each browser resides on a computer with a unique IP.



Downloaded from www.Manualslib.com manuals search engine

Also, IP filtering of proxied administrative sessions has to be based on the IP address of the proxy server rather than the IP address of the computer. This conflicts with administrative session communication that does use the actual IP address of the computer. For more information about IP filtering of administrative sessions, see Access Policy, page 12-11.

For these reasons, we do not recommend performing administrative sessions using a web browser that is configured to use a proxy server. Administrative sessions using a proxy-enabled web browser is not tested. If your web browser is configured to use a proxy server, disable HTTP proxying when attempting Cisco Secure ACS administrative sessions.

## Administrative Sessions through Firewalls

In the case of firewalls that do not perform network address translation (NAT), administrative sessions conducted across the firewall can require additional configuration of Cisco Secure ACS and the firewall. This is because Cisco Secure ACS assigns a random HTTP port at the beginning of an administrative session.

To allow administrative sessions from browsers outside a firewall that protects Cisco Secure ACS, the firewall must permit HTTP traffic across the range of ports that Cisco Secure ACS is configured to use. You can control the HTTP port range using the HTTP port allocation feature. For more information about the HTTP port allocation feature, see HTTP Port Allocation for Administrative Sessions, page 1-23.

While administering Cisco Secure ACS through a firewall that is not performing NAT is possible, we do not recommend that you administer Cisco Secure ACS through a firewall. For more information, see HTTP Port Allocation for Administrative Sessions, page 1-23.

## Administrative Sessions through a NAT Gateway

We do not recommend conducting administrative sessions across a network device performing NAT. If the administrator runs a browser on a computer behind a NAT gateway, Cisco Secure ACS receives the HTTP requests from the public IP address of the NAT device, which conflicts with the computer private IP address, included in the content of the HTTP requests. Cisco Secure ACS does not permit this.



Downloaded from www.Manualslib.com manuals search engine

If Cisco Secure ACS is behind a NAT gateway and the URL used to access the HTML interface specifies Cisco Secure ACS by its hostname, administrative sessions operate correctly, provided that DNS is functioning correctly on your network or that computers used to access the HTML interface have a hosts file entry for Cisco Secure ACS.

If the URL used to access the HTML interface specifies Cisco Secure ACS by its IP address, you could configure the gateway to forward all connections to port 2002 to Cisco Secure ACS, using the same port. Additionally, all the ports allowed using the HTTP port allocation feature would have to be similarly mapped. We have not tested such a configuration and do not recommend implementing it.

# Accessing the HTML Interface

Remote administrative sessions always require that you log in using a valid administrator name and password, as configured in the Administration Control section. If the Allow automatic local login check box is cleared on the Sessions Policy Setup page in the Administration Control section, Cisco Secure ACS requires a valid administrator name and password for administrative sessions accessed from a browser on the computer running Cisco Secure ACS.

**Before You Begin**

Determine whether a supported web browser is installed on the computer you want to use to access the HTML interface. If not, install a supported web browser or use a computer that already has a supported web browser installed. For a list of supported browsers, see the Release Notes. The latest revision to the Release Notes is posted on Cisco.com (http://www.cisco.com).

Because the HTML interface uses Java in a few places, the computer running the browser used to access the HTML interface must have a Java Virtual Machine available for the use of the browser.

To access the HTML interface, follow these steps:

**Step 1** Open a web browser. For a list of supported web browsers, see the Release Notes for the version of Cisco Secure ACS you are accessing. The most recent revision to the Release Notes is posted on Cisco.com (http://www.cisco.com).



Downloaded from www.Manualslib.com manuals search engine

**Step 2** In the Address or Location bar in the web browser, type the applicable URL. For a list of possible URLs, see Uniform Resource Locator for the HTML Interface, page 1-29.

**Step 3** If the Cisco Secure ACS login page appears, follow these steps:

a. In the Username box, type a valid Cisco Secure ACS administrator name.

b. In the Password box, type the password for the administrator name you specified.

c. Click **Login**.

The initial page appears, listing build and copyright information.

# Logging Off the HTML Interface

When you are finished using the HTML interface, we recommend that you log off. While Cisco Secure ACS can timeout unused administrative sessions, logging off prevents unauthorized access by someone using the browser after you or by unauthorized persons using the HTTP port left open to support the administrative session.

To log off the Cisco Secure ACS HTML interface, click the **Logoff** button.

**Note** The Logoff button appears in the upper right corner of the browser window, except on the initial page, where it appears in the upper left of the configuration area.

# Online Help and Online Documentation

We provide two sources of information in the HTML interface:

- **Online Help**—Contains basic information about the page shown in the configuration area.
- **Online Documentation**—Contains the entire user guide.



Downloaded from www.Manualslib.com manuals search engine

## Using Online Help

Online help is the default content in the display area. For every page that appears in the configuration area, there is a corresponding online help page. At the top of each online help page is a list of topics covered by that page.

To jump from the top of the online help page to a particular topic, click the topic name in the list at the top of the page.

There are three icons that appear on many pages in Cisco Secure ACS:

- **Question Mark**—Many subsections of the pages in the configuration area contain an icon with a question mark. To jump to the applicable topic in an online help page, click the question mark icon.
- **Section Information**—Many online help pages contain a Section Information icon at the bottom of the page. To view an applicable section of the online documentation, click the Section Information icon.
- **Back to Help**—Wherever you find a online help page with a Section Information icon, the corresponding page in the configuration area contains a Back to Help icon. If you have accessed the online documentation by clicking a Section Information icon and want to view the online help page again, click the Back to Help icon.

## Using the Online Documentation

Online documentation is the user guide for Cisco Secure ACS. The user guide provides information about the configuration, operation, and concepts of Cisco Secure ACS. The information presented in the online documentation is as current as the release date of the Cisco Secure ACS version you are using. For the most up-to-date documentation about Cisco Secure ACS, please go to http://www.cisco.com

**Tip** Click **Section Information** on any online help page to view online documentation relevant to the section of the HTML interface you are using.



Downloaded from www.Manualslib.com manuals search engine

To access online documentation, follow these steps:

**Step 1** In the Cisco Secure ACS HTML interface, click **Online Documentation**.

**Tip** To open the online documentation in a new browser window, right-click **Online Documentation**, and then click **Open Link in New Window** (for Microsoft Internet Explorer) or **Open in New Window** (for Netscape Navigator).

The table of contents opens in the configuration area.

**Step 2** If you want to select a topic from the table of contents, scroll through the table of contents and click the applicable topic.

The online documentation for the topic selected appears in the display area.

**Step 3** If you want to select a topic from the index, follow these steps:

**a.** Click **[Index]**.

The index appears in the display area.

**b.** Scroll through the index to find an entry for the topic you are researching.

**Tip** Use the lettered shortcut links to jump to a particular section of the index.

Entries appear with numbered links after them. The numbered links lead to separate instances of the entry topic.

**c.** Click an instance number for the desired topic.

The online documentation for the topic selected appears in the display area.

**Step 4** If you want to print the online documentation, click in the display area, and then click **Print** in the navigation bar of your browser.



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

# Deployment Considerations

Deployment of Cisco Secure ACS for Windows Server can be complex and iterative, depending on the specific implementation required. This chapter provides insight into the deployment process and presents a collection of factors that you should consider before deploying Cisco Secure ACS.

The complexity of deploying Cisco Secure ACS reflects the evolution of AAA servers in general, and the advanced capabilities, flexibility, and features of Cisco Secure ACS in particular. AAA was conceived originally to provide a centralized point of control for user access via dial-up services. As user databases grew and the locations of AAA clients became more dispersed, more capability was required of the AAA server. Regional, and then global, requirements became common. Today, Cisco Secure ACS is required to provide AAA services for dial-up access, dial-out access, wireless, VLAN access, firewalls, VPN concentrators, administrative controls, and more. The list of external databases supported has also continued to grow and the use of multiple databases, as well as multiple Cisco Secure ACSes, has become more common. Regardless of the scope of your Cisco Secure ACS deployment, the information contained in this chapter should prove valuable. If you have deployment questions that are not addressed in this guide, contact your Cisco technical representative for assistance.

This chapter contains the following topics:


- Basic Deployment Requirements for Cisco Secure ACS, page 2-2
- Basic Deployment Factors for Cisco Secure ACS, page 2-6
- Suggested Deployment Sequence, page 2-19




Downloaded from www.Manualslib.com manuals search engine

# Basic Deployment Requirements for Cisco Secure ACS

This section details the minimum requirements you must meet to successfully deploy Cisco Secure ACS.

This section contains the following topics:


- System Requirements, page 2-2
  - Hardware Requirements, page 2-2
  - Operating System Requirements, page 2-2
  - Third-Party Software Requirements, page 2-3
- Network and Port Requirements, page 2-4


## System Requirements

The computer running Cisco Secure ACS must meet the minimum hardware and software requirements detailed in the following sections.

### Hardware Requirements

The computer running Cisco Secure ACS must meet the following minimum hardware requirements:

- Pentium III processor, 550 MHz or faster.
- 256 MB of RAM.
- At least 250 MB of free disk space. If you are running your database on the same computer, more disk space is required.
- Minimum graphics resolution of 256 colors at 800 x 600 lines.

### Operating System Requirements

Cisco Secure ACS for Windows Servers 3.3 supports the Windows operating systems listed below. Both the operating system and the service pack must be English-language versions.



Downloaded from www.Manualslib.com manuals search engine

- Windows 2000 Server, with Service Pack 4 installed
- Windows 2000 Advanced Server, with the following conditions:
  - with Service Pack 4 installed
  - without Microsoft clustering service installed
  - without other features specific to Windows 2000 Advanced Server enabled

**Note** We have not tested and cannot support the multi-processor feature of Windows 2000 Advanced Server. Windows 2000 Datacenter Server is not a supported operating system.

- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Standard Edition

Windows service packs can be applied before or after installing Cisco Secure ACS. If you do not install a required service pack before installing Cisco Secure ACS, the Cisco Secure ACS installation program may warn you that the required service pack is not present. If you receive a service pack message, continue the installation, and then install the required service pack before starting user authentication with Cisco Secure ACS.

For the most recent information about tested operating systems and service packs, see the Release Notes. The current version of the Release Notes are on Cisco.com, accessible from the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm

## Third-Party Software Requirements

The Release Notes provide information about third-party software products that we tested with Cisco Secure ACS and that we support, including applications such as:

- Web browsers and Java virtual machines
- Novell NDS clients
- Token-card clients



Downloaded from www.Manualslib.com manuals search engine

Other than the software products described in the Release Notes, we have not tested the interoperability of Cisco Secure ACS and other software products on the same computer. We only support interoperability issues of software products that are mentioned in the Release Notes. The most recent version of the Release Notes are posted on Cisco.com, accessible from the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm

# Network and Port Requirements

Your network should meet the following requirements before you begin deploying Cisco Secure ACS.

- For full TACACS+ and RADIUS support on Cisco IOS devices, AAA clients must run Cisco IOS Release 11.2 or later.
- Non-Cisco IOS AAA clients must be configured with TACACS+ and/or RADIUS.
- Dialin, VPN, or wireless clients must be able to connect to the applicable AAA clients.
- The computer running Cisco Secure ACS must be able to ping all AAA clients.
- Gateway devices between Cisco Secure ACS and other network devices must permit communication over the ports needed to support the applicable feature or protocol. For information about ports that Cisco Secure ACS listens to, see Table 2-1.
- A supported web browser must be installed on the computer running Cisco Secure ACS. For the most recent information about tested browsers, see the Release Notes. The most recent version of the Release Notes are posted on Cisco.com, accessible from the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/index.htm
- All network cards in the computer running Cisco Secure ACS must be enabled. If there is a disabled network card on the computer running Cisco Secure ACS, installing Cisco Secure ACS may proceed slowly due to delays caused by Microsoft CryptoAPI.



Downloaded from www.Manualslib.com manuals search engine

**Note** We tested Cisco Secure ACS on computers that have only one network interface card.

- If you want to have Cisco Secure ACS use the "Grant Dial-in Permission to User" feature in Windows when authorizing network users, this option must be selected in the Windows User Manager or Active Directory Users and Computers for the applicable user accounts.

Table 2-1 lists the ports that Cisco Secure ACS listens to for communications with AAA clients, other Cisco Secure ACSes and applications, and web browsers. Cisco Secure ACS uses other ports to communicate with external user databases; however, it initiates those communications rather than listening to specific ports. In some cases, these ports are configurable, such as with LDAP and RADIUS token server databases. For more information about ports that a particular external user database listens to, see the documentation for that database.

***Table 2-1 Ports that Cisco Secure ACS Listens To***

| Feature/Protocol | UDP or TCP? | Ports |
|---|---|---|
| RADIUS authentication and authorization | UDP | 1645, 1812 |
| RADIUS accounting | UDP | 1646, 1813 |
| TACACS+ | TCP | 49 |
| CiscoSecure Database Replication | TCP | 2000 |
| RDBMS Synchronization with synchronization partners | TCP | 2000 |
| User-Changeable Password web application | TCP | 2000 |
| Logging | TCP | 2001 |
| Administrative HTTP port for new sessions | TCP | 2002 |
| Administrative HTTP port range | TCP | Configurable; default 1024 through 65535 |



Downloaded from www.Manualslib.com manuals search engine

# Basic Deployment Factors for Cisco Secure ACS

Generally, the ease in deploying Cisco Secure ACS is directly related to the complexity of the implementation planned and the degree to which you have defined your policies and requirements. This section presents some basic factors you should consider before you begin implementing Cisco Secure ACS.

This section contains the following topics:


- Network Topology, page 2-6
- Remote Access Policy, page 2-14
- Security Policy, page 2-15
- Administrative Access Policy, page 2-15
- Database, page 2-18
- Network Latency and Reliability, page 2-19


## Network Topology

How your enterprise network is configured is likely to be the most important factor in deploying Cisco Secure ACS. While an exhaustive treatment of this topic is beyond the scope of this guide, this section details how the growth of network topology options has made Cisco Secure ACS deployment decisions more complex.

When AAA was created, network access was restricted to either devices directly connected to the LAN or remote devices gaining access via modem. Today, enterprise networks can be complex and, because of tunneling technologies, can be widely geographically dispersed.

### Dial-Up Topology

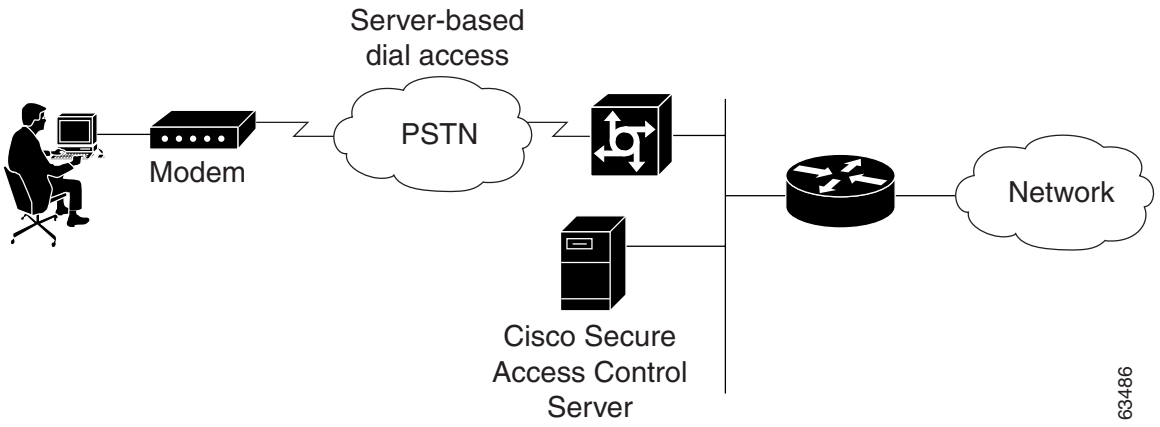
In the traditional model of dial-up access (a PPP connection), a user employing a modem or ISDN connection is granted access to an intranet via a network access server (NAS) functioning as a AAA client. Users may be able to connect via only a single AAA client as in a small business, or have the option of numerous geographically dispersed AAA clients.



Downloaded from www.Manualslib.com manuals search engine

In the small LAN environment, see Figure 2-1, network architects typically place a single Cisco Secure ACS internal to the AAA client, protected from outside access by a firewall and the AAA client. In this environment, the user database is usually small, there are few devices that require access to the Cisco Secure ACS for AAA, and any database replication is limited to a secondary Cisco Secure ACS as a backup.

***Figure 2-1 Small Dial-up Network***

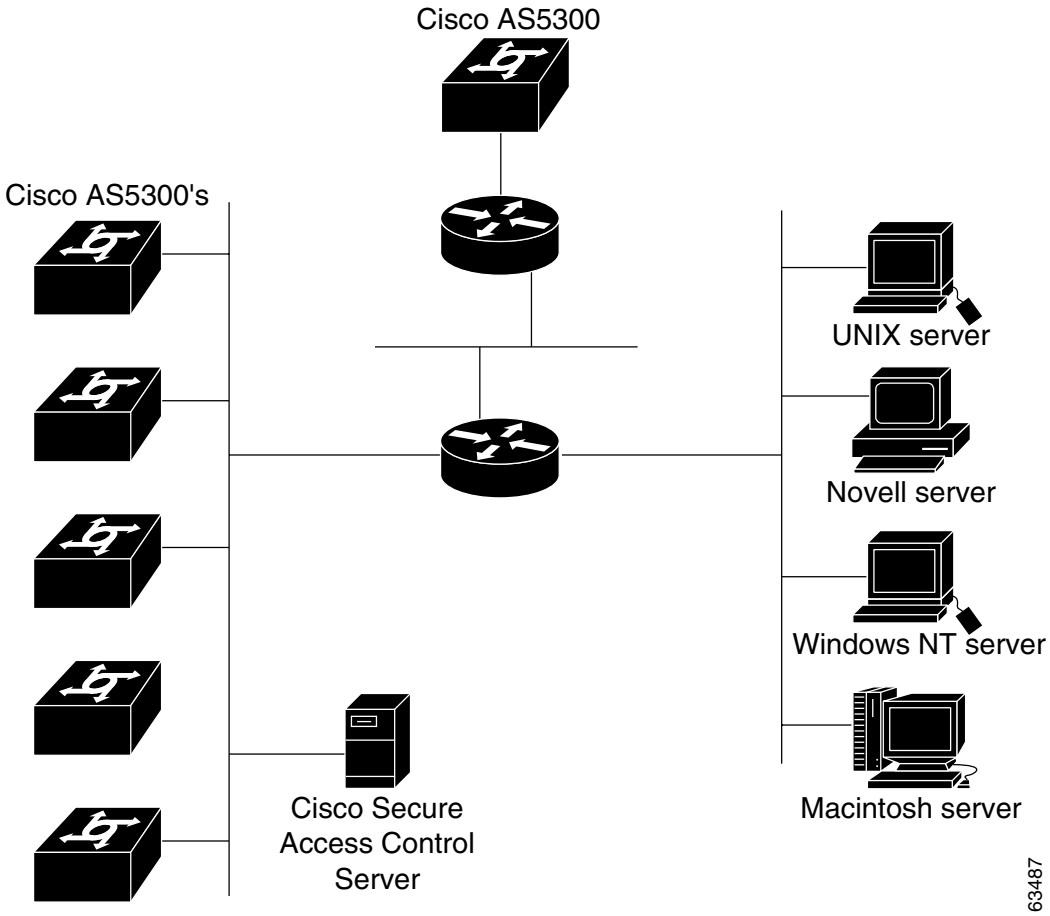



In a larger dial-in environment, a single Cisco Secure ACS with a backup may be suitable, too. The suitability of this configuration depends on network and server access latency. Figure 2-2 shows an example of a large dial-in arrangement. In this scenario the addition of a backup Cisco Secure ACS is a recommended addition.



Downloaded from www.Manualslib.com manuals search engine

*Figure 2-2 Large Dial-up Network*

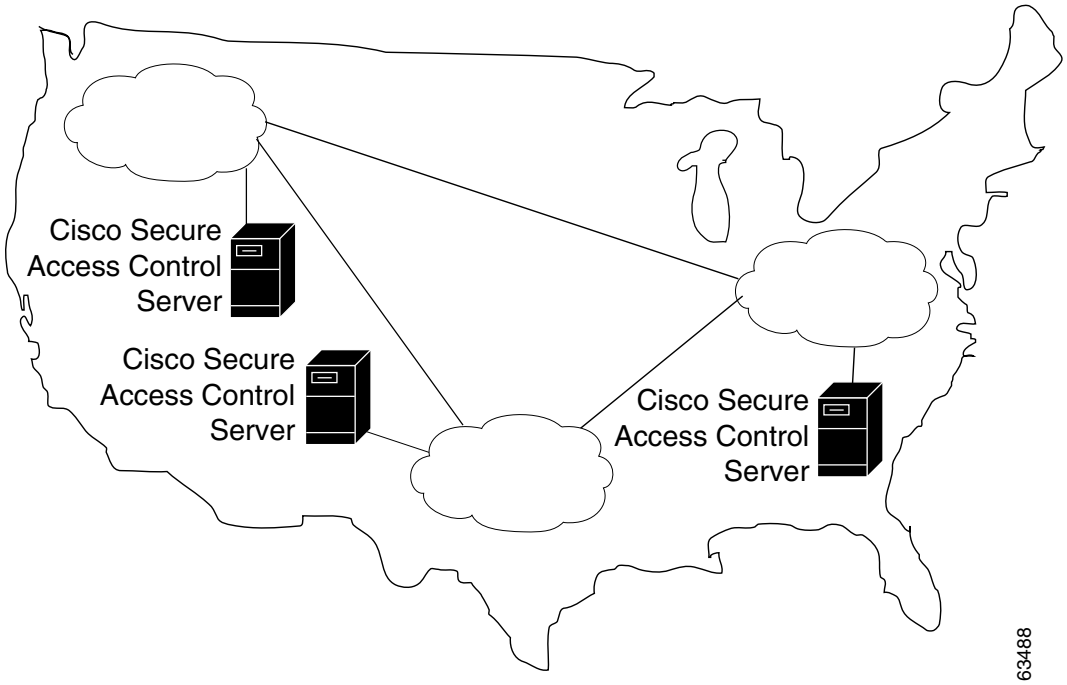



In a very large, geographically dispersed network (Figure 2-3), there may be access servers located in different parts of a city, in different cities, or on different continents. If network latency is not an issue, a central Cisco Secure ACS may work but connection reliability over long distances may cause problems. In this case, local Cisco Secure ACSes may be preferable to a central Cisco Secure ACS. If the need for a globally coherent user database is most important, database replication or synchronization from a central Cisco Secure ACS may be necessary. Authentication using external databases, such as a Windows user database or the Lightweight Directory Access Protocol (LDAP), can further complicate the deployment of distributed, localized Cisco Secure ACSes. While Cisco Secure ACS uses encryption for all replication and database synchronization traffic, additional security measures may be required to protect the network and user information that Cisco Secure ACS sends across the WAN.



Downloaded from www.Manualslib.com manuals search engine

*Figure 2-3 Geographically Dispersed Network*




## Wireless Network

The wireless network access point is a relatively new client for AAA services. The wireless access point (AP), such as the Cisco Aironet series, provides a bridged connection for mobile end-user clients into the LAN. Authentication is absolutely necessary due to the ease of access to the AP. Encryption is also necessary because of the ease of eavesdropping on communications. As such, security plays an even bigger role than in the dial-up scenario and is discussed in more detail later in this section.

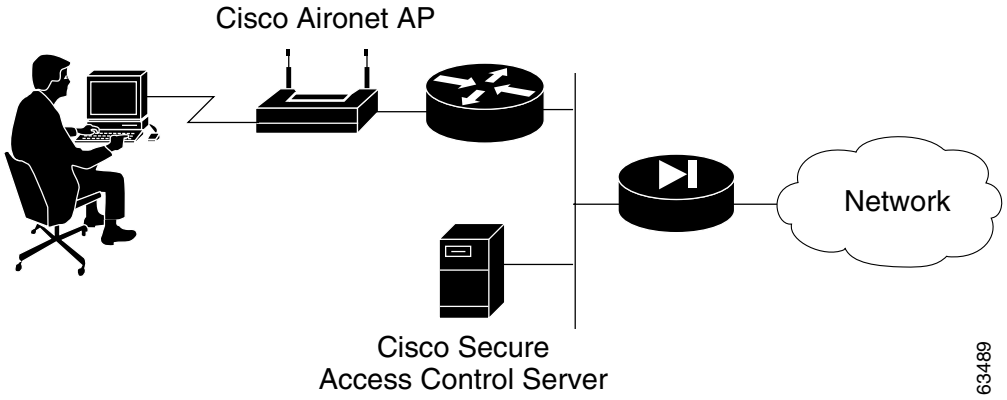
Scaling can be a serious issue in the wireless network. The mobility factor of the wireless LAN (WLAN) requires considerations similar to those given to the dial-up network. Unlike the wired LAN, however, the WLAN can be more readily expanded. Though WLAN technology does have physical limits as to the number of users that can be connected via an AP, the number of APs can grow quickly. As with the dial-up network, you can structure your WLAN to allow full access for all users, or to provide restricted access to different subnets between sites, buildings, floors, or rooms. This raises a unique issue with the WLAN: the ability of a user to “roam” between APs.



Downloaded from www.Manualslib.com manuals search engine

In the simple WLAN, there may be a single AP installed (Figure 2-4). Because there is only one AP, the primary issue is security. In this environment, there is generally a small user base and few network devices to worry about. Providing AAA services to the other devices on the network does not cause any significant additional load on the Cisco Secure ACS.

***Figure 2-4 Simple WLAN***

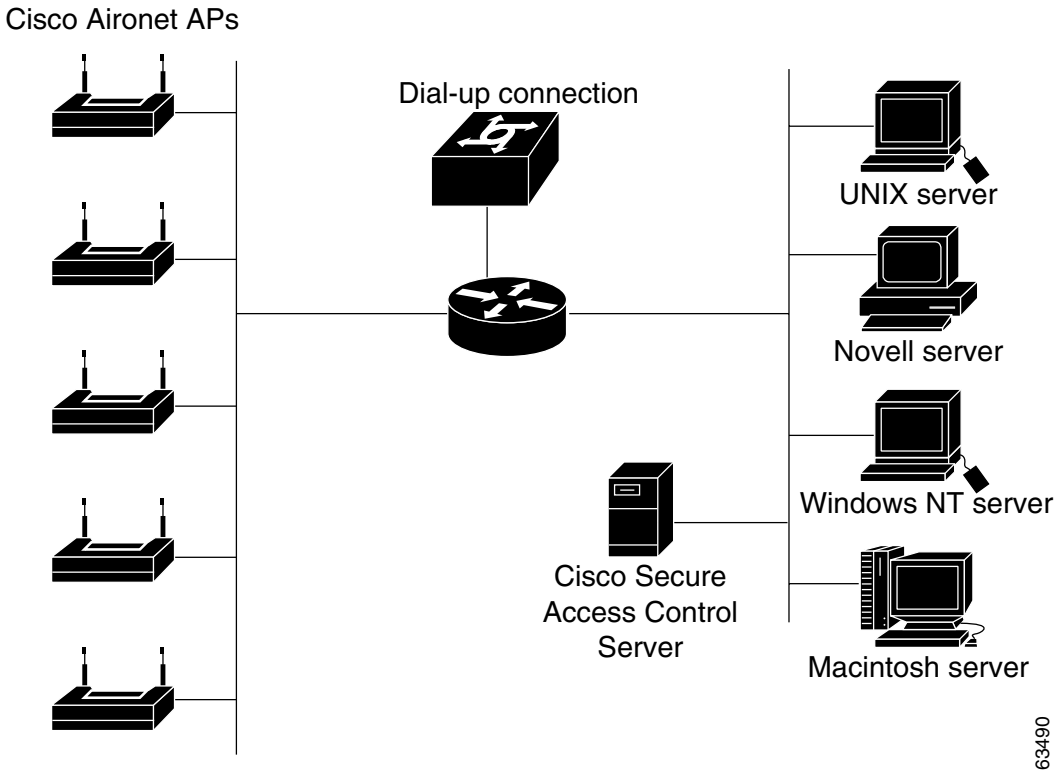



In the LAN where a number of APs are deployed, as in a large building or a campus environment, your decisions on how to deploy Cisco Secure ACS become a little more involved. Though Figure 2-5 shows all APs on the same LAN, they may be distributed throughout the LAN, connected via routers, switches, and so on. In the larger, geographical distribution of WLANs, deployment of Cisco Secure ACS is similar to that of large regional distribution of dial-up LANs (Figure 2-3).



Downloaded from www.Manualslib.com manuals search engine

*Figure 2-5 Campus WLAN*

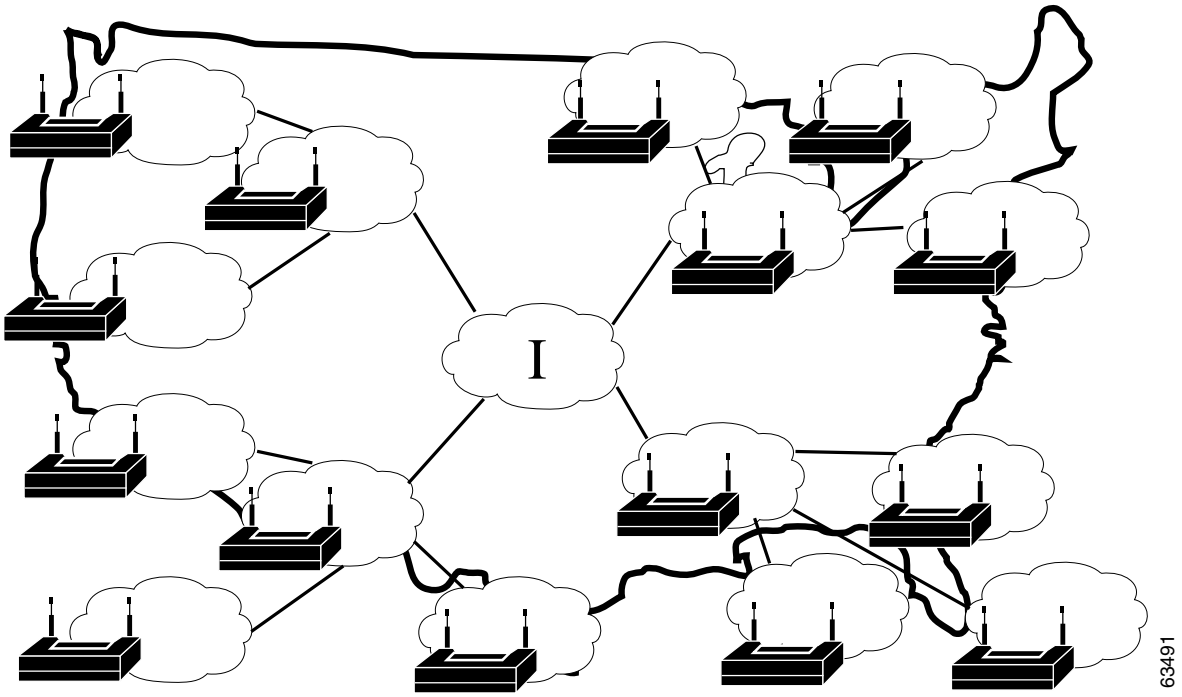



This is particularly true when the regional topology is the campus WLAN. This model starts to change when you deploy WLANs in many small sites that more resemble the simple WLAN shown in Figure 2-4. This model may apply to a chain of small stores distributed throughout a city or state, nationally, or globally (Figure 2-6).



Downloaded from www.Manualslib.com manuals search engine

*Figure 2-6 Large Deployment of Small Sites*




For the model in Figure 2-6, the location of Cisco Secure ACS depends on whether all users need access on any AP, or whether users require only regional or local network access. Along with database type, these factors control whether local or regional Cisco Secure ACSes are required, and how database continuity is maintained. In this very large deployment model, security becomes a more complicated issue, too.

## Remote Access using VPN

Virtual Private Networks (VPNs) use advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets (Figure 2-7). The benefits of a VPN include the following:

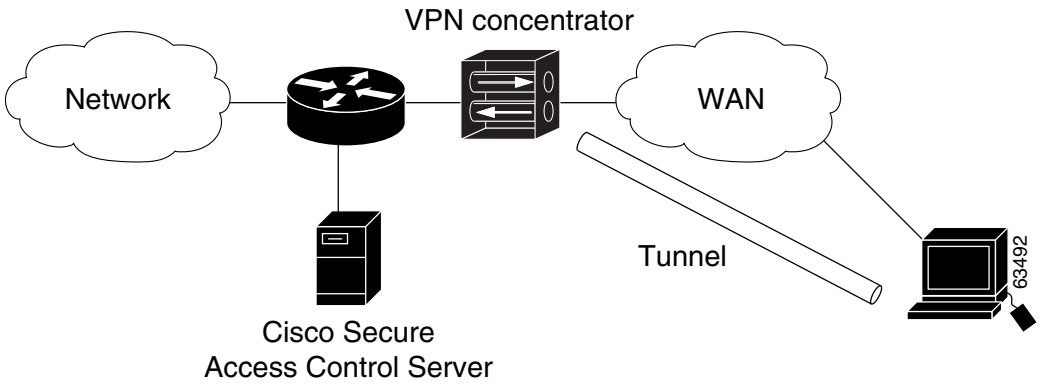
- **Cost Savings**—By leveraging third-party networks with VPN, organizations no longer have to use expensive leased or frame relay lines and can connect remote users to their corporate networks via a local Internet service provider (ISP) instead of using expensive toll-free or long-distance calls to resource-consuming modem banks.



Downloaded from www.Manualslib.com manuals search engine

- **Security**—VPNs provide the highest level of security using advanced encryption and authentication protocols that protect data from unauthorized access.
- **Scalability**—VPNs allow corporations to use remote access infrastructure within ISPs; therefore, corporations can add a large amount of capacity without adding significant infrastructure.
- **Compatibility with Broadband Technology**—VPNs allow mobile workers and telecommuters to take advantage of high-speed, broadband connectivity, such as DSL and cable, when gaining access to their corporate networks, providing workers significant flexibility and efficiency.

***Figure 2-7 Simple VPN Configuration***




There are two types of VPN access into a network:

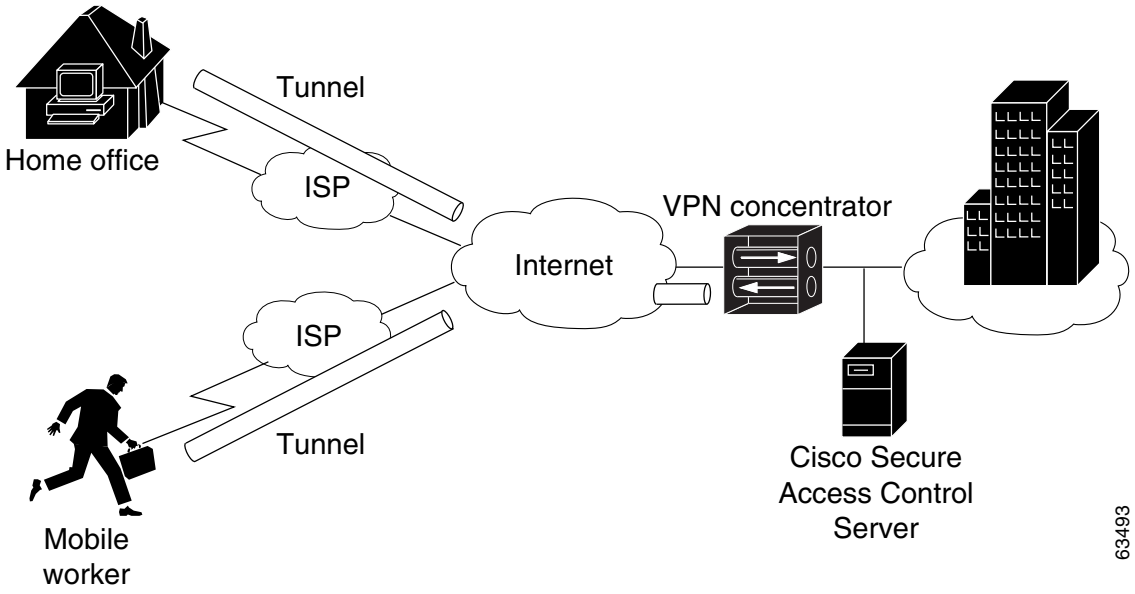
- **Site-to-Site VPNs**—Extend the classic WAN by providing large-scale encryption between multiple fixed sites such as remote offices and central offices, over a public network, such as the Internet.
- **Remote Access VPNs**—Permit secure, encrypted connections between mobile or remote users and their corporate networks via a third-party network, such as an ISP, via VPN client software.

Generally speaking, site-to-site VPNs can be viewed as a typical WAN connection and are not usually configured to use AAA to secure the initial connection and are likely to use the device-oriented IPSec tunneling protocol. Remote access VPNs, however, are similar to classic remote connection technology (modem/ISDN) and lend themselves to using the AAA model very effectively (Figure 2-8).



Downloaded from www.Manualslib.com manuals search engine

*Figure 2-8 Enterprise VPN Solution*




For more information about implementing VPN solutions, see the reference guide *A Primer for Implementing a Cisco Virtual Private Network*.

# Remote Access Policy

Remote access is a broad concept. In general, it defines how the user can connect to the LAN, or from the LAN to outside resources (that is, the Internet). There are several ways this may occur. The methods include dial-in, ISDN, wireless bridges, and secure Internet connections. Each method incurs its own advantages and disadvantages, and provides a unique challenge to providing AAA services. This closely ties remote access policies to the enterprise network topology. In addition to the method of access, other decisions can also affect how Cisco Secure ACS is deployed; these include specific network routing (access lists), time-of-day access, individual restrictions on AAA client access, access control lists (ACLs), and so on.

Remote access policies can be implemented for employees who telecommute or for mobile users who dial in over ISDN or public switched telephone network (PSTN). Such policies are enforced at the corporate campus with Cisco Secure ACS and the AAA client. Inside the enterprise network, remote access policies can control wireless access by individual employees.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS remote access policies provides control by using central authentication and authorization of remote users. The CiscoSecure user database maintains all user IDs, passwords, and privileges. Cisco Secure ACS access policies can be downloaded in the form of ACLs to network access servers such as the Cisco AS5300 Network Access Server, or by allowing access during specific periods, or on specific access servers.

Remote access policies are part of overall corporate security policy.

# Security Policy

We recommend that every organization that maintains a network develop a security policy for the organization. The sophistication, nature, and scope of your security policy directly affect how you deploy Cisco Secure ACS.

For more information about developing and maintaining a comprehensive security policy, refer to the following documents:

- *Network Security Policy: Best Practices White Paper*
- *Delivering End-to-End Security in Policy-Based Networks*
- *Cisco IOS Security Configuration Guide*

# Administrative Access Policy

Managing a network is a matter of scale. Providing a policy for administrative access to network devices depends directly on the size of the network and the number of administrators required to maintain the network. Local authentication on a network device can be performed, but it is not scalable. The use of network management tools can help in large networks, but if local authentication is used on each network device, the policy usually consists of a single login on the network device. This does not promote adequate network device security. Using Cisco Secure ACS allows a centralized administrator database, and administrators can be added or deleted at one location. TACACS+ is the recommended AAA protocol for controlling AAA client administrative access because of its ability to provide per-command control (command authorization) of AAA client administrator access to the device. RADIUS is not well suited for this purpose because of the one-time transfer of authorization information at time of initial authentication.



Downloaded from www.Manualslib.com manuals search engine

The type of access is also an important consideration. If there are to be different administrative access levels to the AAA clients, or if a subset of administrators is to be limited to certain systems, Cisco Secure ACS can be used with command authorization per network device to restrict network administrators as necessary. Using local authentication restricts the administrative access policy to no login on a device or using privilege levels to control access. Controlling access by means of privilege levels is cumbersome and not very scalable. This requires that the privilege levels of specific commands are altered on the AAA client device and specific privilege levels are defined for the user login. It is also very easy to create more problems by editing command privilege levels. Using command authorization on Cisco Secure ACS does not require that you alter the privilege level of controlled commands. The AAA client sends the command to Cisco Secure ACS to be parsed and Cisco Secure ACS determines whether the administrator has permission to use the command. The use of AAA allows authentication on any AAA client to any user on Cisco Secure ACS and limits access to these devices on a per-AAA client basis.

A small network with a small number of network devices may require only one or two individuals to administer it. Local authentication on the device is usually sufficient. If you require more granular control than that which authentication can provide, some means of authorization is necessary. As discussed earlier, controlling access using privilege levels can be cumbersome. Cisco Secure ACS reduces this problem.

In large enterprise networks, with many devices to administer, the use of Cisco Secure ACS becomes a practical necessity. Because administration of many devices requires a larger number of network administrators, with varying levels of access, the use of local control is simply not a viable way of keeping track of network device configuration changes required when changing administrators or devices. The use of network management tools, such as CiscoWorks 2000, helps to ease this burden, but maintaining security is still an issue. Because Cisco Secure ACS can comfortably handle up to 100,000 users, the number of network administrators that Cisco Secure ACS supports is rarely an issue. If there is a large remote access population using RADIUS for AAA support, the corporate IT team should consider separate TACACS+ authentication using Cisco Secure ACS for the administrative team. This would isolate the general user population from the administrative team and reduce the likelihood of inadvertent access to network devices. If this is not a suitable solution, using TACACS+ for administrative (shell/exec) logins, and RADIUS for remote network access, provides sufficient security for the network devices.



Downloaded from www.Manualslib.com manuals search engine

## Separation of Administrative and General Users

It is important to keep the general network user from accessing network devices. Even though the general user may not intend to gain unauthorized access, inadvertent access could accidentally disrupt network access. AAA and Cisco Secure ACS provide the means to separate the general user from the administrative user.

The easiest, and recommended, method to perform such separation is to use RADIUS for the general remote access user and TACACS+ for the administrative user. An issue that arises is that an administrator may also require remote network access, like the general user. If you use Cisco Secure ACS this poses no problem. The administrator can have both RADIUS and TACACS+ configurations in Cisco Secure ACS. Using authorization, RADIUS users can have PPP (or other network access protocols) set as the permitted protocol. Under TACACS+, only the administrator would be configured to allow shell (exec) access.

For example, if the administrator is dialing in to the network as a general user, a AAA client would use RADIUS as the authenticating and authorizing protocol and the PPP protocol would be authorized. In turn, if the same administrator remotely connects to a AAA client to make configuration changes, the AAA client would use the TACACS+ protocol for authentication and authorization. Because this administrator is configured on Cisco Secure ACS with permission for shell under TACACS+, he would be authorized to log in to that device. This does require that the AAA client have two separate configurations on Cisco Secure ACS, one for RADIUS and one for TACACS+. An example of a AAA client configuration under IOS that effectively separates PPP and shell logins follows:

```
aaa new-model
tacacs-server host  ip-address
tacacs-server key  secret-key
radius-server host  ip-address
radius-server key  secret-key
aaa authentication ppp default group radius
aaa authentication login default group tacacs+ local
aaa authentication login console none
aaa authorization network default group radius
aaa authorization exec default group tacacs+ none
aaa authorization command 15 default group tacacs+ none
username  user  password  password
line con 0
login authentication console
```



Downloaded from www.Manualslib.com manuals search engine

Conversely, if a general user attempts to use his or her remote access to log in to a network device, Cisco Secure ACS checks and approves the username and password, but the authorization process would fail because that user would not have credentials that allow shell or exec access to the device.

# Database

Aside from topological considerations, the user database is one of the most influential factors involved in making deployment decisions for Cisco Secure ACS. The size of the user base, distribution of users throughout the network, access requirements, and type of user database contribute to how Cisco Secure ACS is deployed.

## Number of Users

Cisco Secure ACS is designed for the enterprise environment, comfortably handling 100,000 users. This is usually more than adequate for a corporation. In an environment that exceeds these numbers, the user base would typically be geographically dispersed, which lends itself to the use of more than one Cisco Secure ACS configuration. A WAN failure could render a local network inaccessible because of the loss of the authentication server. In addition to this issue, reducing the number of users that a single Cisco Secure ACS handles improves performance by lowering the number of logins occurring at any given time and by reducing the load on the database itself.

## Type of Database

Cisco Secure ACS supports several database options, including the CiscoSecure user database or using remote authentication with any of the external databases supported. For more information about database options, types, and features, see Authentication and User Databases, page 1-10, Chapter 13, “User Databases”, or Chapter 16, “User Group Mapping and Specification”. Each database option has its own advantages and limitations in scalability and performance.



Downloaded from www.Manualslib.com manuals search engine

# Network Latency and Reliability

Network latency and reliability are also important factors in how you deploy Cisco Secure ACS. Delays in authentication can result in timeouts at the end-user client or the AAA client.

The general rule for large, extended networks, such as a globally dispersed corporation, is to have at least one Cisco Secure ACS deployed in each region. This may not be adequate without a reliable, high-speed connection between sites. Many corporations use secure VPN connections between sites so that the Internet provides the link. This saves time and money but it does not provide the speed and reliability that a dedicated frame relay or T1 link provides. If reliable authentication service is critical to business functionality, such as retail outlets with cash registers that are linked by a WLAN, the loss of WAN connection to a remote Cisco Secure ACS could be catastrophic.

The same issue can be applied to an external database used by Cisco Secure ACS. The database should be deployed close enough to Cisco Secure ACS to ensure reliable and timely access. Using a local Cisco Secure ACS with a remote database can result in the same problems as using a remote Cisco Secure ACS. Another possible problem in this scenario is that a user may experience timeout problems. The AAA client would be able to contact Cisco Secure ACS, but Cisco Secure ACS would wait for a reply that might be delayed or never arrive from the external user database. If the Cisco Secure ACS were remote, the AAA client would time out and try an alternative method to authenticate the user, but in the latter case, it is likely the end-user client would time out first.

# Suggested Deployment Sequence

While there is no single process for all Cisco Secure ACS deployments, you should consider following the sequence, keyed to the high-level functions represented in the navigation toolbar. Also bear in mind that many of these deployment activities are iterative in nature; you may find that you repeatedly return to such tasks as interface configuration as your deployment proceeds.

- **Configure Administrators**—You should configure at least one administrator at the outset of deployment; otherwise, there is no remote administrative access and all configuration activity must be done from the server. You should also have a detailed plan for establishing and maintaining an administrative policy.



Downloaded from www.Manualslib.com manuals search engine

For more information about setting up administrators, see Chapter 1, "Overview".

- **Configure the Cisco Secure ACS HTML Interface**—You can configure the Cisco Secure ACS HTML interface to show only those features and controls that you intend to use. This makes using Cisco Secure ACS less difficult than it would be if you had to contend with multiple parts of the HTML interface that you do not plan to use. The price of this convenience can sometimes be frustration that features and controls do not appear because you failed to configure them in the Interface Configuration section. For guidance on configuring the HTML interface, see Interface Design Concepts, page 3-2.

  For information about configuring particular aspects of the HTML interface, see the following sections of the interface configuration chapter:

  - User Data Configuration Options, page 3-3
  - Advanced Options, page 3-4
  - Protocol Configuration Options for TACACS+, page 3-7
  - Protocol Configuration Options for RADIUS, page 3-11

- **Configure System**—There are more than a dozen functions within the System Configuration section to be considered, from setting the format for the display of dates and password validation to configuring settings for database replication and RDBMS synchronization. These functions are detailed in Chapter 8, "System Configuration: Basic". Of particular note during initial system configuration is setting up the logs and reports to be generated by Cisco Secure ACS; for more information, see Chapter 1, "Overview".

- **Configure Network**—You control distributed and proxied AAA functions in the Network Configuration section of the HTML interface. From here, you establish the identity, location, and grouping of AAA clients and servers, and determine what authentication protocols each is to use. For more information, see Chapter 4, "Network Configuration".

- **Configure External User Database**—During this phase of deployment you must decide whether and how you intend to implement an external database to establish and maintain user authentication accounts. Typically, this decision is made according to your existing network administration mechanisms. For information about the types of databases Cisco Secure ACS supports and instructions for establishing them, see Chapter 13, "User Databases".



Downloaded from www.Manualslib.com manuals search engine

Along with the decision to implement an external user database (or databases), you should have detailed plans that specify your requirements for Cisco Secure ACS database replication, backup, and synchronization. These aspects of configuring CiscoSecure user database management are detailed in Chapter 8, "System Configuration: Basic".

- **Configure Shared Profile Components**—With most aspects of network configuration already established and before configuring user groups, you should configure your Shared Profile Components. When you set up and name the network access restrictions and command authorization sets you intend to employ, you lay out an efficient basis for specifying user group and single user access privileges. For more information about Shared Profile Components, see Chapter 5, "Shared Profile Components".
- **Configure Groups**—Having previously configured any external user databases you intend to employ, and before configuring your user groups, you should decide how to implement two other Cisco Secure ACS features related to external user databases: unknown user processing and database group mapping. For more information, see About Unknown User Authentication, page 15-4 and Chapter 16, "User Group Mapping and Specification". Then, you can configure your user groups with a complete plan of how Cisco Secure ACS is to implement authorization and authentication. For more information, see Chapter 6, "User Group Management".
- **Configure Users**—With groups established, you can establish user accounts. Remember that a particular user can belong to only one user group, and that settings made at the user level override settings made at the group level. For more information, see Chapter 7, "User Management".
- **Configure Reports**—Using the Reports and Activities section of the Cisco Secure ACS HTML interface, you can specify the nature and scope of logging that Cisco Secure ACS performs. For more information, see Chapter 1, "Overview".



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

# Interface Configuration

Ease of use is the overriding design principle of the HTML interface in the Cisco Secure ACS for Windows Server. Cisco Secure ACS presents intricate concepts of network security from the perspective of an administrator. The Interface Configuration section of Cisco Secure ACS enables you to configure the Cisco Secure ACS HTML interface—you can tailor the interface to simplify the screens you will use by hiding the features that you do not use and by adding fields for your specific configuration.

**Note** We recommend that you return to this section to review and confirm your initial settings. While it is logical to begin your Cisco Secure ACS configuration efforts with configuring the interface, sometimes a section of the HTML interface that you initially believed should be hidden from view may later require configuration from within this section.

**Tip** If a section of the Cisco Secure ACS HTML interface appears to be "missing" or "broken", return to the Interface Configuration section and confirm that the particular section has been activated.

This chapter contains the following topics:


- Interface Design Concepts, page 3-2
- User Data Configuration Options, page 3-3
- Advanced Options, page 3-4




Downloaded from www.Manualslib.com manuals search engine

- Protocol Configuration Options for TACACS+, page 3-7
- Protocol Configuration Options for RADIUS, page 3-11

# Interface Design Concepts

Before you begin to configure the Cisco Secure ACS HTML interface for your particular configuration, you should understand a few basic precepts of the system operation. The information in the following sections is necessary for effective interface configuration.

## User-to-Group Relationship

A user can belong to only one group at a time. As long as there are no conflicting attributes, users inherit group settings.

**Note** If a user profile has an attribute configured differently from the same attribute in the group profile, the user setting always overrides the group setting.

If a user has a unique configuration requirement, you can make that user a part of a group and set unique requirements on the User Setup page, or you can assign that user to his or her own group.

## Per-User or Per-Group Features

You can configure most features at both group and user levels, with the following exceptions:

- **User level only**—Static IP address, password, and expiration.
- **Group level only**—Password aging and time-of-day/day-of-week restrictions.



Downloaded from www.Manualslib.com manuals search engine

# User Data Configuration Options

The Configure User Defined Fields page enables you to add (or edit) up to five fields for recording information on each user. The fields you define in this section subsequently appear in the Supplementary User Information section at the top of the User Setup page. For example, you could add the user's company name, telephone number, department, billing code, and so on. You can also include these fields in the accounting logs. For more information about the accounting logs, see About Cisco Secure ACS Logs and Reports, page 11-6. For information on the data fields that compose the user data options, see User-Defined Attributes, page F-34.

## Defining New User Data Fields

To configure new user data fields, follow these steps:

**Step 1** Click **Interface Configuration**, and then click **User Data Configuration**.

The Configure User Defined Fields page appears. Check boxes in the Display column indicate which fields are configured to appear in the Supplementary User Information section at the top of the User Setup page.

**Step 2** Select a check box in the Display column.

**Step 3** In the corresponding Field Title box, type a title for the new field.

**Step 4** To configure another field, repeat Step 2 and Step 3.

**Step 5** When you have finished configuring new user data fields, click **Submit**.

**Tip** You can change the title of a field by editing the text in the Field Title box and then clicking Submit. For the change to take effect, you must restart the Cisco Secure ACS services by clicking Restart at the bottom of the Service Control page in the System Configuration section and then stopping and restarting the CSAdmin service by using the Services section of the Administrative Tools folder in Windows Control Panel.



Downloaded from www.Manualslib.com manuals search engine

Restarting Cisco Secure ACS-related Windows services should be done during off hours because it briefly interrupts authentication, authorization, and accounting.

# Advanced Options

The Advanced Options page enables you to determine which advanced features Cisco Secure ACS displays. You can simplify the pages displayed in other areas of the Cisco Secure ACS HTML interface by hiding advanced features that you do not use.

**Caution** Disabling an advanced feature in the Interface Configuration section does not affect anything except the display of that feature in the HTML interface. Settings made while an advanced feature was displayed remain in effect when that advanced feature is no longer displayed. Further, the interface displays any advanced feature that has non-default settings, even if you have configured that advanced feature to be hidden. If you later disable the feature or delete its settings, Cisco Secure ACS hides the advanced feature. The only exception is the Network Device Groups feature. Regardless of whether Network Device Groups are in use, they are hidden when deselected on the Advanced Options page.

The advanced option features include the following:

- **Per-User TACACS+/RADIUS Attributes**—When selected, this feature enables TACACS+/RADIUS attributes to be set at a per-user level, in addition to being set at the group level.
- **User-Level Shared Network Access Restrictions**—When selected, this feature enables the Shared Profile Component network access restrictions (NARs) options on the User Setup page. These options allow you to apply previously configured, named, IP-based and CLID/DNIS-based NARs at the user level. For information on defining a NAR, or NAR set, within Shared Profile Components, see Adding a Shared Network Access Restriction, page 5-19.



Downloaded from www.Manualslib.com manuals search engine

- **User-Level Network Access Restrictions**—When selected, this feature enables the two sets of options for defining user-level, IP-based and CLI/DNIS-based NARs on the User Setup page.
- **User-Level Downloadable ACLs**—When selected, this feature enables the Downloadable ACLs (access control lists) section on the User Setup page.
- **Default Time-of-Day/Day-of-Week Specification**—When selected, this feature enables the default time-of-day/day-of-week access settings grid on the Group Setup page.
- **Group-Level Shared Network Access Restrictions**—When selected, this feature enables the Shared Profile Component NAR options on the Group Setup page. These options allow you to apply previously configured, named, IP-based and CLID/DNIS-based NARs at the group level. For information on defining a NAR, or NAR set, within Shared Profile Components, see Adding a Shared Network Access Restriction, page 5-19.
- **Group-Level Network Access Restrictions**—When selected, this feature enables the two sets of options for defining group-level, IP-based and CLI/DNIS-based NARs on the Group Setup page.
- **Group-Level Downloadable ACLs**—When selected, this feature enables the Downloadable ACLs section on the Group Setup page.
- **Group-Level Password Aging**—When selected, this feature enables the Password Aging section on the Group Setup page. The Password Aging feature enables you to force users to change their passwords.
- **Max Sessions**—When selected, this feature enables the Max Sessions section on the User Setup and Group Setup pages. The Max Sessions option sets the maximum number of simultaneous connections for a group or a user.
- **Usage Quotas**—When selected, this feature enables the Usage Quotas sections on the User Setup and Group Setup pages. The Usage Quotas option sets one or more quotas for usage by a group or a user.
- **Distributed System Settings**—When selected, this feature displays the AAA server and proxy tables on the Network Interface page. If the tables have information other than the defaults in them, they always appear.
- **Remote Logging**—When selected, this feature enables the Remote Logging feature on the Logging page of the System Configuration section.
- **Cisco Secure ACS Database Replication**—When selected, this feature enables the Cisco Secure ACS database replication information on the System Configuration page.



Downloaded from www.Manualslib.com manuals search engine

- **RDBMS Synchronization**—When selected, this feature enables the RDBMS (Relational Database Management System) Synchronization option on the System Configuration page. If RDBMS Synchronization is configured, this option always appears.
- **IP Pools**—When selected, this feature enables the IP Pools Address Recovery and IP Pools Server options on the System Configuration page.
- **Network Device Groups**—When selected, this option enables network device groups (NDGs). When NDGs are enabled, the Network Configuration section and parts of the User Setup and Group Setup pages change to enable you to manage groups of network devices (AAA clients or AAA servers). This feature is useful if you have many devices to administer.
- **Voice-over-IP (VoIP) Group Settings**—When selected, this feature enables the VoIP option on the Group Setup page.
- **Voice-over-IP (VoIP) Accounting Configuration**—When selected, this feature enables the VoIP Accounting Configuration option on the System Configuration page. This option is used to determine the logging format of RADIUS VoIP accounting packets.
- **ODBC Logging**—When selected, this feature enables the ODBC logging sections on the Logging page of the System Configuration section.

# Setting Advanced Options for the Cisco Secure ACS User Interface

To set advanced options for the Cisco Secure ACS HTML interface, follow these steps:

**Step 1** Click **Interface Configuration**, and then click **Advanced Options**.

The Advanced Options table appears.

**Step 2** Select each option that you want displayed (enabled) in the Cisco Secure ACS HTML interface.

**Caution** Disabling an advanced feature in the Interface Configuration section does not affect anything except the display of that feature in the HTML interface. Settings made while an advanced feature was displayed remain in effect when that



Downloaded from www.Manualslib.com manuals search engine

advanced feature is no longer displayed. Further, the interface displays any advanced feature that has non-default settings, even if you have configured that advanced feature to be hidden. If you later disable the feature or delete its settings, Cisco Secure ACS hides the advanced feature. The only exception is the Network Device Groups feature. Regardless of whether Network Device Groups are in use, they are hidden when deselected on the Advanced Options page.

**Step 3** When you have finished making selections, click **Submit**.

Cisco Secure ACS alters the contents of various sections of the HTML interface according to the selections you have made.

# Protocol Configuration Options for TACACS+

The TACACS+ (Cisco) page details the configuration of the Cisco Secure ACS HTML interface for TACACS+ settings. The interface settings enable you to display or hide TACACS+ administrative and accounting options. You can simplify the HTML interface by hiding the features that you do not use.

The TACACS+ (Cisco) page comprises three distinct areas, as follows:

**Tip** The default interface setting presents a single column of check boxes, at the group level only, for selecting TACACS+ Services Settings and New Service Settings. To view two columns of check boxes that enable you to configure settings at the Group level or the User level, you must have enabled the Per-user TACACS+/RADIUS Attributes option on the Advanced Options page of Interface Configuration section.

- **TACACS+ Services Settings**—In this area is a list of the most commonly used services and protocols for TACACS+. You select each TACACS+ service that you want to appear as a configurable option on either the User Setup page or Group Setup page.
- **New Services**—In this area you can enter any services or protocols particular to your network configuration.



Downloaded from www.Manualslib.com manuals search engine

**Note** If you have configured Cisco Secure ACS to interact with device management applications for other Cisco products, such as Management Center for Firewalls, Cisco Secure ACS may display new TACACS+ services as dictated by these device management applications. To ensure the proper functioning of Cisco Secure ACS, of device management applications with which Cisco Secure ACS interacts, and of the Cisco network devices managed by those applications, do not change or delete automatically generated TACACS+ service types.

- **Advanced Configuration Options**—In this area you can add more detailed information for even more tailored configurations.

  The four items you can choose to hide or display are as follows:

  - **Advanced TACACS+ Features**—This option displays or hides the Advanced TACACS+ Options section on the User Setup page. These options include Privilege Level Authentication and Outbound Password Configuration for SENDPASS and SENDAUTH clients, such as routers.
  - **Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings**—If this option is selected, a grid appears on the User Setup page that enables you to override the TACACS+ scheduling attributes on the Group Setup page.

    You can control the use of each TACACS+ service by the time of day and day of week. For example, you can restrict Exec (Telnet) access to business hours but permit PPP-IP access at any time.

    The default setting is to control time-of-day access for all services as part of authentication. However, you can override the default and display a time-of-day access grid for every service. This keeps user and group setup easy to manage, while making this feature available for the most sophisticated environments. This feature applies only to TACACS+ because TACACS+ can separate the authentication and authorization processes. RADIUS time-of-day access applies to all services. If TACACS+ and RADIUS are used simultaneously, the default time-of-day access applies to both. This provides a common method to control access regardless of the access control protocol.



Downloaded from www.Manualslib.com manuals search engine

– **Display a window for each service selected in which you can enter customized TACACS+ attributes**—If this option is selected, an area appears on the User Setup and Group Setup pages that enables you to enter custom TACACS+ attributes.

  Cisco Secure ACS can also display a custom command field for each service. This text field enables you to make specialized configurations to be downloaded for a particular service for users in a particular group.

  You can use this feature to send many TACACS+ commands to the access device for the service, provided that the device supports the command, and that the command syntax is correct. This feature is disabled by default, but you can enable it the same way you enable attributes and time-of-day access.

– **Display enable Default (Undefined) Service Configuration**—If this check box is selected, an area appears on the User Setup and Group Setup pages that enables you to permit unknown TACACS+ services, such as Cisco Discovery Protocol (CDP).

**Note** This option should be used by advanced system administrators only.

**Note** Customized settings at the user level take precedence over settings at the group level.

# Setting Options for TACACS+

This procedure enables you to display or hide TACACS+ administrative and accounting options. It is unlikely that you will use every service and protocol available for TACACS+. Displaying each would make setting up a user or group cumbersome. To simplify setup, you can use the TACACS+ (Cisco IOS) Edit page to customize the services and protocols that appear.



Downloaded from www.Manualslib.com manuals search engine

To configure the user interface for TACACS+ options, follow these steps:

**Note** The Cisco Secure ACS HTML interface displays any protocol option that is enabled or has non-default values, even if you have configured that protocol option to be hidden. If you later disable the option or delete its value and the protocol option is configured to be hidden, Cisco Secure ACS hides the protocol option. This behavior prevents Cisco Secure ACS from hiding active settings.

**Step 1** Click **Interface Configuration**, and then click **TACACS+ (Cisco IOS)**.

The TACACS+ (Cisco) page appears.

**Step 2** In the TACACS+ Services table, select the check box for each TACACS+ service you want displayed on the applicable setup page.

**Step 3** To add new services and protocols, follow these steps:

**a.** In the New Services section of the TACACS+ Services table, type in any Service and Protocol to be added.

**Note** If you have configured Cisco Secure ACS to interact with device management applications for other Cisco products, such as a Management Center for Firewalls, Cisco Secure ACS may display new TACACS+ services as dictated by these device management applications. To ensure the proper functioning of Cisco Secure ACS, of device management applications with which Cisco Secure ACS interacts, and of the Cisco network devices managed by those applications, do not change or delete automatically generated TACACS+ service types.

**b.** Select the appropriate check box to select those that should be displayed for configuration either under User Setup, or Group Setup, or both.

**Step 4** In the Advanced Configurations Options section, select the check boxes of the display options you want to enable.

**Step 5** When you have finished setting TACACS+ interface display options, click **Submit**.



Downloaded from www.Manualslib.com manuals search engine

The selections made in this procedure determine what TACACS+ options Cisco Secure ACS displays in other sections of the HTML interface.

# Protocol Configuration Options for RADIUS

It is unlikely that you would want to install every attribute available for every protocol. Displaying each would make setting up a user or group cumbersome. To simplify setup, this section allows you to customize the attributes that are displayed. For a list of supported RADIUS AV pairs and accounting AV pairs, see Appendix C, "RADIUS Attributes".

Depending on which AAA client or clients you have configured, the Interface Configuration page displays different types of RADIUS protocol configuration settings choices. The Interface Configuration page displays RADIUS IETF settings whenever any RADIUS AAA client is configured. The Interface Configuration page also displays additional settings for each vendor-specific RADIUS type. The settings that appear for various types of AAA client depend on what settings that type of device can employ. These combinations are detailed in Table 3-1 on page 3-12.



Downloaded from www.Manualslib.com manuals search engine

*Table 3-1 RADIUS Listings in Interface*

| Configure this Type of AAA Client... | ...the Interface Configuration Page Lists the Types of Settings Shown | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | RADIUS (IETF) | RADIUS (Cisco Aironet) | RADIUS (BBSM) | RADIUS (Cisco IOS/PIX) | RADIUS (Micro-soft) | RADIUS (Ascend) | RADIUS (Cisco VPN 3000) | RADIUS (Cisco VPN 5000) | RADIUS (Juniper) | RADIUS (Nortel) |
| **RADIUS (IETF)** | Yes | No | No | No | No | No | No | No | No | No |
| **RADIUS (Cisco Aironet)** | Yes | Yes | No | Yes | No | No | No | No | No | No |
| **RADIUS (BBSM)** | Yes | No | Yes | No | No | No | No | No | No | No |
| **RADIUS (Cisco IOS/PIX)** | Yes | No | No | Yes | Yes | Yes | No | No | No | No |



Downloaded from www.Manualslib.com manuals search engine

*Table 3-1 RADIUS Listings in Interface (continued)*

| Configure this Type of AAA Client... | ...the Interface Configuration Page Lists the Types of Settings Shown | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | RADIUS (IETF) | RADIUS (Cisco Aironet) | RADIUS (BBSM) | RADIUS (Cisco IOS/PIX) | RADIUS (Microsoft) | RADIUS (Ascend) | RADIUS (Cisco VPN 3000) | RADIUS (Cisco VPN 5000) | RADIUS (Juniper) | RADIUS (Nortel) |
| **RADIUS (Ascend)** | Yes | No | No | No | Yes | Yes | No | No | No | No |
| **RADIUS (Cisco VPN 3000)** | Yes | No | No | Yes | Yes | No | Yes | No | No | No |
| **RADIUS (Cisco VPN 5000)** | Yes | No | No | No | No | No | No | Yes | No | No |
| **RADIUS (Juniper)** | Yes | No | No | No | No | No | No | No | Yes | No |
| **RADIUS (Nortel)** | Yes | No | No | No | No | No | No | No | No | Yes |
| **RADIUS (iPass)** | Yes | No | No | No | No | No | No | No | No | No |

**Tip** You must have your network devices configured before you can select, on the Interface Configuration page, a type of setting for further configuration.

From the Interface Configuration page, when you select a type of RADIUS setting to configure, the HTML interface displays the corresponding list of available RADIUS attributes and associated check boxes. If you have selected the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options, a User check box appears alongside the Group check box for each attribute. Otherwise, only the Group check box for each attribute appears. By



Downloaded from www.Manualslib.com manuals search engine

selecting check boxes in a list of attributes, you determine whether the corresponding (IETF) RADIUS attribute or vendor-specific attribute (VSA) is configurable from the User Setup and Group Setup sections.

Details regarding the types of RADIUS settings pages follow:

- **(IETF) RADIUS Settings**—This page lists attributes available for (IETF) RADIUS.

  These standard (IETF) RADIUS attributes are available for any network device configuration when using RADIUS. If you want to use IETF attribute number 26 (for VSAs), select Interface Configuration and then RADIUS for the vendors whose network devices you use. Attributes for (IETF) RADIUS and the VSA for each RADIUS network device vendor supported by Cisco Secure ACS appear in User Setup or Group Setup.

  **Note** The RADIUS (IETF) attributes are shared with RADIUS VSAs. You must configure the first RADIUS attributes from RADIUS (IETF) for the RADIUS vendor.

  The Tags to Display Per Attribute option (located under Advanced Configuration Options) enables you to specify how many values to display for tagged attributes on the User Setup and Group Setup pages. Examples of tagged attributes include [064]Tunnel-Type and [069]Tunnel-Password.

  For detailed steps, see Setting Protocol Configuration Options for IETF RADIUS Attributes, page 3-16.

- **RADIUS (Cisco IOS/PIX) Settings**—This section allows you to enable the specific attributes for RADIUS (Cisco IOS/PIX). Selecting the first attribute listed under RADIUS (Cisco IOS/PIX), 026/009/001, displays an entry field under User Setup and/or Group Setup in which any TACACS+ commands can be entered to fully leverage TACACS+ in a RADIUS environment. For detailed steps, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17.

- **RADIUS (Cisco Aironet) Settings**—This section allows you to enable the specific attribute for RADIUS (Cisco Aironet). The single Cisco Aironet RADIUS VSA, Cisco-Aironet-Session-Timeout, is a specialized implementation of the IETF RADIUS Session-Timeout attribute (27). When Cisco Secure ACS responds to an authentication request from a Cisco Aironet Access Point and the Cisco-Aironet-Session-Timeout attribute is configured, Cisco Secure ACS sends to the wireless device this value in the IETF



Downloaded from www.Manualslib.com manuals search engine

Session-Timeout attribute. This enables you to provide different session timeout values for wireless and wired end-user clients. For detailed steps, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17.

- **RADIUS (Ascend) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Ascend). This page appears if you have configured a RADIUS (Ascend) or a RADIUS (Cisco IOS/PIX) device. For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17.
- **RADIUS (Cisco VPN 3000) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Cisco VPN 3000). For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17.
- **RADIUS (Cisco VPN 5000) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Cisco VPN 5000). For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17.
- **RADIUS (Microsoft) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Microsoft). This page appears if you configure a RADIUS (Ascend), or a RADIUS (VPN 3000), or a RADIUS (Cisco IOS/PIX) device. For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17.
- **RADIUS (Nortel) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Nortel). For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17.
- **RADIUS (Juniper) Settings**—From this section you enable the RADIUS VSAs for RADIUS (Juniper). For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17.
- **RADIUS (BBSM) Settings**—From this section you enable the RADIUS VSAs for RADIUS "Building Broadband Service Manger" (BBSM). For detailed procedures, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17.

While Cisco Secure ACS ships with these listed VSAs prepackaged, it also enables you to define and configure custom attributes for any VSA set not already contained in Cisco Secure ACS. If you have configured a custom VSA and a corresponding AAA client, from the Interface Configuration section you can select the custom VSA and then set the options for how particular attributes



Downloaded from www.Manualslib.com manuals search engine

appear as configurable options on the User Setup or Group Setup page. For information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-28.

# Setting Protocol Configuration Options for IETF RADIUS Attributes

This procedure enables you to hide or display any of the standard IETF RADIUS attributes for configuration from other portions of the Cisco Secure ACS HTML interface.

**Note** If the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options is selected, a User check box appears alongside the Group check box for each attribute.

**Note** Each selected IETF RADIUS attribute must be supported by all your network devices using RADIUS.

To set protocol configuration options for IETF RADIUS attributes, follow these steps:

**Step 1** Click **Interface Configuration**, and then click **RADIUS (IETF)**.

The RADIUS (IETF) page appears.

**Step 2** For each IETF RADIUS attribute that you want to appear as a configurable option on the User Setup or Group Setup page, select the corresponding check box.

**Note** Each attribute selected must be supported by your RADIUS network devices.

**Step 3** To specify how many values to display for tagged attributes on the User Setup and Group Setup pages, select the **Tags to Display Per Attribute** option, and then select a value from the corresponding list. Examples of tagged attributes are `[064] Tunnel-Type` and `[069] Tunnel-Password`.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** When you have finished selecting the attributes, click **Submit** at the bottom of the page.

Each IETF RADIUS attribute that you selected appears as a configurable option on the User Setup or Group Setup page, as applicable.

# Setting Protocol Configuration Options for Non-IETF RADIUS Attributes

This procedure enables you to hide or display various RADIUS VSAs for configuration from the User Setup and Group Setup portions of the Cisco Secure ACS HTML interface.

To set protocol configuration options for a set of RADIUS VSAs, follow these steps:

**Step 1** Click **Interface Configuration**.

**Step 2** Click one of the RADIUS VSA set types displayed, for example, `RADIUS (Ascend)`.

The page listing the selected set of available RADIUS VSAs appears.

**Note** If the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options is selected, a User check box appears alongside the Group check box for each attribute.

**Step 3** For each RADIUS VSA that you want to appear as a configurable option on the User Setup or Group Setup page, select the corresponding check box.

**Note** Each attribute selected must be supported by your RADIUS network devices.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** Click **Submit** at the bottom of the page.

According to your selections, the RADIUS VSAs appear on the User Setup or Group Setup pages, or both, as a configurable option.



Downloaded from www.Manualslib.com manuals search engine

# Network Configuration

This chapter details concepts and procedures for configuring Cisco Secure ACS for Windows Server to interact with AAA clients and servers and for establishing a distributed system.

This chapter contains the following topics:


- About Network Configuration, page 4-1
- About Distributed Systems, page 4-2
- Proxy in Distributed Systems, page 4-4
- Network Device Searches, page 4-8
- AAA Client Configuration, page 4-11
- AAA Server Configuration, page 4-21
- Network Device Group Configuration, page 4-28
- Proxy Distribution Table Configuration, page 4-34


## About Network Configuration

The appearance of the page you see when you click Network Configuration differs according to the network configuration selections you made in the Interface Configuration section. The four tables that may appear in this section are as follows:

- **AAA Clients**—This table lists each AAA client that is configured on the network, together with its IP address and associated protocol.



Downloaded from www.Manualslib.com manuals search engine

If you are using network device groups (NDGs), this table does not appear on the initial page, but is accessed through the Network Device Group table. For more information about this interface configuration, see Advanced Options, page 3-4.

- **AAA Servers**—This table lists each AAA server that is configured on the network together with its IP address and associated type.

  If you are using NDGs, this table does not appear on the initial page, but is accessed through the Network Device Groups table. For more information about this interface configuration, see Advanced Options, page 3-4.

- **Network Device Groups**—This table lists the name of each NDG that has been configured, and the number of AAA clients and AAA servers assigned to each NDG. If you are using NDGs, the AAA Clients table and AAA Servers table do not appear on the opening page. To configure a AAA client or AAA server, you must click the name of the NDG to which the device is assigned. If the newly configured device is not assigned to an NDG, it belongs to the (Not Assigned) group.

  This table appears only when you have configured the interface to use NDGs. For more information about this interface configuration, see Advanced Options, page 3-4.

- **Proxy Distribution Table**—You can use the Proxy Distribution Table to configure proxy capabilities including “domain” stripping. For more information, see Proxy Distribution Table Configuration, page 4-34.

  This table appears only when you have configured the interface to enable Distributed Systems Settings. For more information about this interface configuration, see Advanced Options, page 3-4.

# About Distributed Systems

Cisco Secure ACS can be used in a distributed system; that is, multiple Cisco Secure ACSes and authentication, authorization, and accounting (AAA) servers can be configured to communicate with one another as primary, backup, client, or peer systems. This enables you to use powerful features such as the following:

- Proxy
- Fallback on failed connection



Downloaded from www.Manualslib.com manuals search engine

- CiscoSecure database replication
- Remote and centralized logging

# AAA Servers in Distributed Systems

"AAA server" is the generic term for an access control server (ACS), and the two terms are often used interchangeably. AAA servers are used to determine who can access the network and what services are authorized for each user. The AAA server stores a profile containing authentication and authorization information for each user. Authentication information validates user identity, and authorization information determines what network services a user is permitted to use. A single AAA server can provide concurrent AAA services to many dial-up access servers, routers, and firewalls. Each network device can be configured to communicate with a AAA server. This makes it possible to centrally control dial-up access, and to secure network devices from unauthorized access.

These types of access control have unique authentication and authorization requirements. With Cisco Secure ACS, system administrators can use a variety of authentication methods that are used with different degrees of authorization privileges.

Completing the AAA functionality, Cisco Secure ACS serves as a central repository for accounting information. Each user session granted by Cisco Secure ACS can be fully accounted for, and its accounting information can be stored in the server. This accounting information can be used for billing, capacity planning, and security audits.

**Note** If the fields mentioned in this section do not appear in the Cisco Secure ACS HTML interface, enable them by clicking **Interface Configuration**, clicking **Advanced Options**, and then selecting the **Distributed System Settings** check box.

# Default Distributed System Settings

You use both the AAA Servers table and the Proxy Distribution Table to establish distributed system settings. The parameters configured within these tables create the foundation to enable multiple Cisco Secure ACSes to be configured to work



Downloaded from www.Manualslib.com manuals search engine

with one another. Each table contains a Cisco Secure ACS entry for itself. In the AAA Servers table, the only AAA server initially listed is itself; the Proxy Distribution Table lists an initial entry of `(Default)`, which displays how the local Cisco Secure ACS is configured to handle each authentication request locally.

You can configure additional AAA servers in the AAA Servers table. This enables these devices to become available in the HTML interface so that they can be configured for other distributed features such as proxy, CiscoSecure user database replication, remote logging, and RDBMS synchronization. For information about configuring additional AAA servers, see Adding a AAA Server, page 4-24.

# Proxy in Distributed Systems

Proxy is a powerful feature that enables you to use Cisco Secure ACS for authentication in a network that uses more than one AAA server. Using proxy, Cisco Secure ACS automatically forwards an authentication request from a AAA client to another AAA server. After the request has been successfully authenticated, the authorization privileges that have been configured for the user on the remote AAA server are passed back to the original Cisco Secure ACS, where the AAA client applies the user profile information for that session.

Proxy provides a useful service to users, such as business travelers, who dial in to a network device other than the one they normally use and would otherwise be authenticated by a "foreign" AAA server. To use proxy, you must first click **Interface Configuration**, click **Advanced Options**, and then select the **Distributed System Settings** check box.

Whether, and where, an authentication request is to be forwarded is defined in the Proxy Distribution Table on the Network Configuration page. You can use multiple Cisco Secure ACSes throughout your network. For information about configuring the Proxy Distribution Table, see Proxy Distribution Table Configuration, page 4-34.

Cisco Secure ACS employs character strings defined by the administrator to determine whether an authentication request should be processed locally or forwarded, and to where. When an end user dials in to the network device and Cisco Secure ACS finds a match for the character string defined in the Proxy Distribution Table, Cisco Secure ACS forwards the authentication request to the associated remote AAA server.



Downloaded from www.Manualslib.com manuals search engine

**Note** When a Cisco Secure ACS receives a TACACS+ authentication request forwarded by proxy, any Network Access Restrictions for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

**Note** When a Cisco Secure ACS proxies to a second Cisco Secure ACS, the second Cisco Secure ACS responds to the first using only IETF attributes, no VSAs, when it recognizes the first Cisco Secure ACS as a AAA server. Alternatively, you can configure an Cisco Secure ACS to be seen as a AAA client by the second Cisco Secure ACS; in this case, the second Cisco Secure ACS responses include the RADIUS VSAs for whatever RADIUS vendor is specified in the AAA client definition table entry—in the same manner as any other AAA client.

For example, a Cisco Secure ACS receives an authentication request for mary.smith@corporate.com, where "@corporate.com" is a character string defined in the server distribution table as being associated with another specific AAA server. The Cisco Secure ACS receiving the authentication request for mary.smith@corporate.com then forwards the request to the AAA server with which that character string is associated. The entry in the Proxy Distribution Table defines the association.

Administrators with geographically dispersed networks can configure and manage the user profiles of employees within their immediate location or building. This enables the administrator to manage the policies of just their users and allows all authentication requests from other users within the company to be forwarded to their respective AAA server for authentication. Not every user profile needs to reside on every AAA server. This saves administration time and server space, and facilitates end users receiving the same privileges regardless of which access device they connect through.

# Fallback on Failed Connection

You can configure the order in which Cisco Secure ACS checks remote AAA servers when a failure of the network connection to the primary AAA server has occurred. If an authentication request cannot be sent to the first listed server, because of a network failure for example, the next listed server is checked. This



Downloaded from www.Manualslib.com manuals search engine

continues, in order, down the list until a AAA server handles the authentication request. (Failed connections are detected by failure of the nominated server to respond within a specified time period. That is, the request is timed out.) If Cisco Secure ACS cannot connect to any server in the list, authentication fails.

### Character String

Cisco Secure ACS forwards authentication requests using a configurable set of characters with a delimiter, such as dots (.), slashes (/), or hyphens (-). When configuring the Cisco Secure ACS character string to match, you must specify whether the character string is the prefix or suffix. For example, you can use "domain.us" as a suffix character string in username*domain.us, where * represents any delimiter. An example of a prefix character string is domain.*username, where the * would be used to detect the "/" character.

### Stripping

Stripping allows Cisco Secure ACS to remove, or strip, the matched character string from the username. When you enable stripping, Cisco Secure ACS examines each authentication request for matching information. When Cisco Secure ACS finds a match by character string in the Proxy Distribution Table, as described in the example under Proxy in Distributed Systems, page 4-4, Cisco Secure ACS strips off the character string if you have configured it to do so. For example, in the proxy example that follows, the character string that accompanies the username establishes the ability to forward the request to another AAA server. If the user must enter the user ID of mary@corporate.com to be forwarded correctly to the AAA server for authentication, Cisco Secure ACS might find a match on the "@corporate.com" character string, and strip the "@corporate.com", leaving a username of "mary", which may be the username format that the destination AAA server requires to identify the correct entry in its database.

## Proxy in an Enterprise

This section presents a scenario of proxy used in an enterprise system. Mary is an employee with an office in the corporate headquarters in Los Angeles. Her username is mary@la.corporate.com. When Mary needs access to the network, she accesses the network locally and authenticates her username and password.



Downloaded from www.Manualslib.com manuals search engine

Because Mary works in the Los Angeles office, her user profile, which defines her authentication and authorization privileges, resides on the local Los Angeles AAA server. However, Mary occasionally travels to a division within the corporation in New York, where she still needs to access the corporate network to get her e-mail and other files. When Mary is in New York, she dials in to the New York office and logs in as mary@la.corporate.com. Her username is not recognized by the New York Cisco Secure ACS, but the Proxy Distribution Table contains an entry, "@la.corporate.com", to forward the authentication request to the Los Angeles Cisco Secure ACS. Because the username and password information for Mary reside on that AAA server, when she authenticates correctly, the authorization parameters assigned to her are applied by the AAA client in the New York office.

# Remote Use of Accounting Packets

When proxy is employed, Cisco Secure ACS can dispatch AAA accounting packets in one of three ways:

- Log them locally.
- Forward them to the destination AAA server.
- Log them locally and forward copies to the destination AAA server.

Sending accounting packets to the remote Cisco Secure ACS offers several benefits. When Cisco Secure ACS is configured to send accounting packets to the remote AAA server, the remote AAA server logs an entry in the accounting report for that session on the destination server. Cisco Secure ACS also caches the user connection information and adds an entry in the List Logged on Users report. You can then view the information for users that are currently connected. Because the accounting information is being sent to the remote AAA server, even if the connection fails, you can view the Failed Attempts report to troubleshoot the failed connection.

Sending the accounting information to the remote AAA server also enables you to use the Max Sessions feature. The Max Sessions feature uses the Start and Stop records in the accounting packet. If the remote AAA server is a Cisco Secure ACS and the Max Sessions feature is implemented, you can track the number of sessions allowed for each user or group.



Downloaded from www.Manualslib.com manuals search engine

You can also choose to have Voice-over-IP (VoIP) accounting information logged remotely, either appended to the RADIUS Accounting log, in a separate VoIP Accounting log, or both.

## Other Features Enabled by System Distribution

Beyond basic proxy and fallback features, configuring a Cisco Secure ACS to interact with distributed systems enables several other features that are beyond the scope of this chapter. These features include the following:

- **Replication**—For more information, see CiscoSecure Database Replication, page 9-1.
- **RDBMS synchronization**—For more information, see RDBMS Synchronization, page 9-25.
- **Remote and centralized logging**—For more information, see Remote Logging, page 11-26.

# Network Device Searches

You can search for any network device configured in the Network Configuration section of the Cisco Secure ACS HTML interface.

This section contains the following topics:

- Network Device Search Criteria, page 4-8
- Searching for Network Devices, page 4-9

## Network Device Search Criteria

You can specify search criteria for network device searches. Cisco Secure ACS provides the following search criteria:

- **Name**—The name assigned to the network device in Cisco Secure ACS. You can use asterisks (*) as wildcard characters. For example, if you wanted to find all devices with names starting with the letter M, you would enter “M*”



Downloaded from www.Manualslib.com manuals search engine

or “m*”. Name-based searches are case insensitive. If you do not want to search based on device name, you can leave the Name box blank or you can put only an asterisk in the Name box.

- **IP Address**—The IP address specified for the network device in Cisco Secure ACS. For each octet in the address, you have three options, as follows:
  - **Number**—You can specify a number, for example, 10.3.157.98.
  - **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen, for example, 10.3.157.10-50.
  - **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

  Cisco Secure ACS allows any octet or octets in the IP Address box to be a number, a numeric range, or an asterisk, for example 172.16-31.*.*.
- **Type**—The device type, as specified by the AAA protocol it is configured to use, or the kind of AAA server it is. If you do not want to limit the search based on device type, select `Any` from the Type list.
- **Device Group**—The NDG the device is assigned to. This search criterion only appears if you have enabled Network Device Groups on the Advanced Options page in the Interface Configuration section. If you do not want to limit the search based on NDG membership, select `Any` from the Device Group list.

# Searching for Network Devices

To search for a network device, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** Click **Search**.

The Search for Network Devices page appears. In the configuration area, the controls for setting search criteria appear above the search results for the most recent search previously conducted for this session, if any.



Downloaded from www.Manualslib.com manuals search engine

**Tip** When you leave the Search for Network Devices page, Cisco Secure ACS retains your search criteria and results for the duration of the current administrative session. Until you log out of Cisco Secure ACS, you can return to the Search for Network Devices page to view your most recent search criteria and results.

**Step 3** Set the criteria for a device search. For information about search criteria, see Network Device Search Criteria, page 4-8.

**Tip** To reset the search criteria to default settings, click **Clear**.

**Step 4** Click **Search**.

A table lists each network device configured in Cisco Secure ACS that matches the search criteria you specified. If Cisco Secure ACS did not find a matching network device, the message "No Search Results" appears.

The table listing matching network devices includes the device name, IP address, and type. If you have enabled Network Device Groups on the Advanced Options page in the Interface Configuration Section, the table also includes the NDG of each matching network device.

**Tip** You can sort the table rows by whichever column you like, in either ascending or descending order. Click a column title once to sort the rows by the entries in that column in ascending order. Click the column a second time to sort the rows by the entries in that column in descending order.

**Step 5** If you want to view the configuration settings for a network device found by the search, click the network device name in the Name column of the table of matching network devices.

Cisco Secure ACS displays the applicable setup page. For information about the AAA Client Setup page, see AAA Client Configuration Options, page 4-11. For information about the AAA Server Setup page, see AAA Server Configuration Options, page 4-22.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** If you want to download a file containing the search results in a comma-separated value format, click **Download** and use your browser to save the file to a location and filename of your choice.

**Step 7** If you want to search again using different criteria, repeat Step 3 and Step 4.

# AAA Client Configuration

In this guide we use the term "AAA client" comprehensively to signify the device through which or to which service access is being attempted. This is the RADIUS or TACACS+ client device, and may comprise network access servers (NASes), PIX Firewalls, routers, or any other RADIUS or TACACS+ hardware/software client.

This section contains the following topics:


- AAA Client Configuration Options, page 4-11
- Adding a AAA Client, page 4-16
- Editing a AAA Client, page 4-19
- Deleting a AAA Client, page 4-21


## AAA Client Configuration Options

A AAA client configuration enables Cisco Secure ACS to interact with the network devices the configuration represents. A network device that does not have a corresponding configuration in Cisco Secure ACS, or whose configuration in Cisco Secure ACS is incorrect, does not receive AAA services from Cisco Secure ACS.

The Add AAA Client and AAA Client Setup pages include the following options:

- **AAA Client Hostname**—The name you assign to the AAA client configuration. Each AAA client configuration can represent multiple network devices; thus, the AAA client hostname configured in Cisco Secure ACS is not required to match the hostname configured on a network device. We



Downloaded from www.Manualslib.com manuals search engine

recommend that you adopt a descriptive, consistent naming convention for AAA client hostnames. Maximum length for a AAA client hostname is 32 characters.

**Note** After you submit the AAA client hostname, you cannot change it. If you want to use a different name for a AAA client, delete the AAA client configuration and create a AAA client configuration using the new name.

- **AAA Client IP Address**—At a minimum, a single IP address of a AAA client or the keyword "dynamic".

  If you only use the keyword "dynamic", with no IP addresses, the AAA client configuration can only be used for command authorization for Cisco multi-device management applications, such as Management Center for Firewalls. Cisco Secure ACS only provides AAA services to devices based on IP address, so it ignores such requests from a device whose AAA client configuration only has the keyword "dynamic" in the Client IP Address box.

  If you want a AAA client configuration in Cisco Secure ACS to represent multiple network devices, you can specify multiple IP addresses. Separate each IP address by pressing Enter.

  In each IP address you specify, you have three options for each octet in the address, as follows:

  - **Number**—You can specify a number, for example, 10.3.157.98.
  - **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen, for example, 10.3.157.10-50.
  - **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

  Cisco Secure ACS allows any octet or octets in the IP Address box to be a number, a numeric range, or an asterisk, for example 172.16-31.*.*.

- **Key**—The shared secret of the AAA client. Maximum length for a AAA client key is 32 characters.



Downloaded from www.Manualslib.com manuals search engine

For correct operation, the key must be identical on the AAA client and Cisco Secure ACS. Keys are case sensitive. Because shared secrets are not synchronized, it is easy to make mistakes when entering them on network devices and Cisco Secure ACS. If the shared secret does not match, Cisco Secure ACS discards all packets from the network device.

**Note** If the AAA client represents multiple network devices, the key must be identical on all network devices represented by the AAA client.

- **Network Device Group**—The name of the NDG to which this AAA client should belong. To make the AAA client independent of NDGs, use the Not Assigned selection.

  **Note** This option does not appear if you have not configured Cisco Secure ACS to use NDGs. To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

- **Authenticate Using**—The AAA protocol to be used for communications with the AAA client. The Authenticate Using list includes Cisco IOS TACACS+ and several vendor-specific implementations of RADIUS. If you have configured user-defined RADIUS vendors and VSAs, those vendor-specific RADIUS implementations appear on the list also. For information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-28.

  The Authenticate Using list always contains the following selections:

  - **TACACS+ (Cisco IOS)**—The Cisco IOS TACACS+ protocol, which is the standard choice when using Cisco Systems access servers, routers, and firewalls. If the AAA client is a Cisco device-management application, such as Management Center for Firewalls, you must use this option.
  - **RADIUS (Cisco Aironet)**—RADIUS using Cisco Aironet VSAs. Select this option if the network device is a Cisco Aironet Access Point used by users authenticating with LEAP or EAP-TLS, provided that these protocols are enabled on the Global Authentication Setup page in the System Configuration section.



Downloaded from www.Manualslib.com manuals search engine

When an authentication request from a RADIUS (Cisco Aironet) AAA client arrives, Cisco Secure ACS first attempts authentication by using LEAP; if this fails, Cisco Secure ACS fails over to EAP-TLS. If LEAP is not enabled on the Global Authentication Setup page, Cisco Secure ACS immediately attempts EAP-TLS authentication. If neither LEAP nor EAP-TLS are enabled on the Global Authentication Setup, any authentication attempt received from a Cisco Aironet RADIUS client fail. For more information about enabling LEAP or EAP-TLS, see Global Authentication Setup, page 10-26.

Using this option enables Cisco Secure ACS to send the wireless network device a different session timeout value for user sessions than Cisco Secure ACS sends to wired end-user clients.

**Note** If all authentication requests from a particular Cisco Aironet Access Point are PEAP or EAP-TLS requests, use RADIUS (IETF) instead of RADIUS (Cisco Aironet). Cisco Secure ACS cannot support PEAP authentication using the RADIUS (Cisco Aironet) protocol.

- **RADIUS (Cisco BBMS)**—RADIUS using Cisco BBMS VSAs. Select this option if the network device is a Cisco BBMS network device supporting authentication via RADIUS.
- **RADIUS (Cisco IOS/PIX)**—RADIUS using Cisco IOS/PIX VSAs. This option enables you to pack commands sent to a Cisco IOS AAA client. The commands are defined in the Group Setup section. Select this option for RADIUS environments in which key TACACS+ functions are required to support Cisco IOS equipment.
- **RADIUS (Cisco VPN 3000)**—RADIUS using Cisco VPN 3000 VSAs. Select this option if the network device is a Cisco VPN 3000 series Concentrator.
- **RADIUS (Cisco VPN 5000)**—RADIUS using Cisco VPN 5000 VSAs. Select this option if the network device is a Cisco VPN 5000 series Concentrator.
- **RADIUS (IETF)**—IETF-standard RADIUS, using no VSAs. Select this option if the AAA client represents RADIUS-enabled devices from more than one manufacturer and you want to use standard IETF RADIUS



Downloaded from www.Manualslib.com manuals search engine

attributes. If the AAA client represents a Cisco Aironet Access Point used only by users authenticating with PEAP or EAP-TLS, this is also the protocol to select.

- **RADIUS (Ascend)**—RADIUS using Ascend RADIUS VSAs. Select this option if the network device is an Ascend network device supporting authentication via RADIUS.
- **RADIUS (Juniper)**—RADIUS using Juniper RADIUS VSAs. Select this option if the network device is a Juniper network device supporting authentication via RADIUS.
- **RADIUS (Nortel)**—RADIUS using Nortel RADIUS VSAs. Select this option if the network device is a Nortel network device supporting authentication via RADIUS.
- **RADIUS (iPass)**—RADIUS for AAA clients using iPass RADIUS. Select this option if the network device is an iPass network device supporting authentication via RADIUS. iPass RADIUS is identical to IETF RADIUS.

- **Single Connect TACACS+ AAA Client (Record stop in accounting on failure)**—If you select TACACS+ (Cisco IOS) from the Authenticate Using list, you can use this option to specify that Cisco Secure ACS use a single TCP connection for all TACACS+ communication with the AAA client, rather than a new one for every TACACS+ request. In single connection mode, multiple requests from a network device are multiplexed over a single TCP session. By default, this check box is not selected.

**Note** If TCP connections between Cisco Secure ACS and the AAA client are unreliable, do not use this feature.

- **Log Update/Watchdog Packets from this AAA Client**—Enables logging of update, or watchdog, packets. Watchdog packets are interim packets sent periodically during a session. They provide you with an approximate session length if a AAA client fails and, therefore, no stop packet is received to mark the end of the session. By default, this check box is not selected.
- **Log RADIUS Tunneling Packets from this AAA Client**—Enables logging of RADIUS tunneling accounting packets. Packets are recorded in the RADIUS Accounting reports of Reports and Activity. By default, this check ox is not selected.



Downloaded from www.Manualslib.com manuals search engine

- **Replace RADIUS Port info with Username from this AAA Client**—Enables use of username rather than port number for session state tracking. This option is useful when the AAA client cannot provide unique port values, such as a gateway GPRS support node (GGSN). For example, if you use the Cisco Secure ACS IP pools server and the AAA client does not provide unique port for each user, Cisco Secure ACS assumes that a reused port number indicates that the previous user session has ended and Cisco Secure ACS may reassign the IP address previously assigned to the session with the non-unique port number. By default, this check box is not selected.

**Note** If this option is enabled, Cisco Secure ACS cannot determine the number of user sessions for each user. Each session uses the same session identifier, the username; therefore, the Max Sessions feature is ineffective for users accessing the network through a AAA client with this feature enabled.

# Adding a AAA Client

You can use this procedure to add a AAA client configuration.

**Before You Begin**

For descriptions of the options available while adding a AAA client configuration, see AAA Client Configuration Options, page 4-11.

For Cisco Secure ACS to provide AAA services to a AAA client, you must ensure that gateway devices between AAA clients and Cisco Secure ACS allow communication over the ports needed to support the applicable AAA protocol (RADIUS or TACACS+). For information about ports used by AAA protocols, see AAA Protocols—TACACS+ and RADIUS, page 1-6.

To add a AAA client, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA client is to be assigned. Then, click **Add Entry** below the AAA Clients table.
- To add a AAA client when you have not enabled NDGs, click **Add Entry** below the AAA Clients table.

The Add AAA Client page appears.

**Step 3** In the AAA Client Hostname box, type the name assigned to this AAA client (up to 32 characters).

**Step 4** In the AAA Client IP Address box, do one of the following:

- Type the AAA client IP address or addresses. For information about using wildcards, octet ranges, or multiple IP address, see AAA Client Configuration Options, page 4-11.
- If the AAA client configuration will only be used for command authorization of Cisco multi-device management applications, type **dynamic**.

**Note** If you only provide the keyword “dynamic”, the AAA client configuration cannot be used by Cisco Secure ACS to provide AAA services to a network device and is used solely for command authorization of Cisco multi-device management applications, such as Management Center for Firewalls.

**Step 5** In the Key box, type the shared secret that the AAA client and Cisco Secure ACS use to encrypt the data (up to 32 characters).

**Note** For correct operation, the identical key must be configured on the AAA client and Cisco Secure ACS. Keys are case sensitive.

**Step 6** If you are using NDGs, from the Network Device Group list, select the name of the NDG to which this AAA client should belong, or select **Not Assigned** to set this AAA client to be independent of NDGs.

**Note** If you want to enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.



Downloaded from www.Manualslib.com manuals search engine

**Step 7** From the Authenticate Using list, select the network security protocol used by the AAA client.

**Tip** If you are uncertain which protocol to select on the Authenticate Using list, see AAA Client Configuration Options, page 4-11.

**Step 8** If you want to enable a single connection from a AAA client, rather than a new one for every TACACS+ request, select the **Single Connect TACACS+ AAA Client (Record stop in accounting on failure)** check box.

**Note** If TCP connections between Cisco Secure ACS and the AAA client are unreliable, do not use this feature.

**Step 9** If you want to enable logging of watchdog packets, select the **Log Update/Watchdog Packets from this AAA Client** check box.

**Step 10** If you want to enable logging of RADIUS tunneling accounting packets, select the **Log RADIUS tunneling Packets from this AAA Client** check box.

**Step 11** If you want to track session state by username rather than port number, select the **Replace RADIUS Port info with Username from this AAA** check box.

**Note** If this option is enabled, Cisco Secure ACS cannot determine the number of user sessions for each user. Each session uses the same session identifier, the username; therefore, the Max Sessions feature is ineffective for users accessing the network through a AAA client with this feature enabled.

**Step 12** If you want to save your changes and apply them immediately, click **Submit + Restart**.

**Note** Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter.



Downloaded from www.Manualslib.com manuals search engine

**Tip** If you want to save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

# Editing a AAA Client

You can use this procedure to edit the settings for a AAA client configuration.

**Note** You cannot directly edit the name of a AAA client; rather, you must delete the AAA client entry and then re-establish the entry with the corrected name. For steps about deleting a AAA client configuration, see Deleting a AAA Client, page 4-21. For steps about creating a AAA client configuration, see Adding a AAA Client, page 4-16.

### Before You Begin

For descriptions of the options available while editing a AAA client configuration, see AAA Client Configuration Options, page 4-11.

For Cisco Secure ACS to provide AAA services to a AAA client, you must ensure that gateway devices between AAA clients and Cisco Secure ACS permit communication over the ports needed to support the applicable AAA protocol (RADIUS or TACACS+). For information about ports used by AAA protocols, see AAA Protocols—TACACS+ and RADIUS, page 1-6.

To edit a AAA client, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the name of the AAA client.
- To edit a AAA client when you have not enabled NDGs, click the name of the AAA client in the AAA Client Hostname column of the AAA Clients table.

The AAA Client Setup For *Name* page appears.

**Step 3** Modify the AAA client settings, as needed. For information about the configuration options available for a AAA client, see AAA Client Configuration Options, page 4-11.

**Note** You cannot directly edit the name of a AAA client; rather, you must delete the AAA client entry and then re-establish the entry with the corrected name. For steps about deleting a AAA client entry, see Deleting a AAA Client, page 4-21. For steps about creating a AAA client entry, see Adding a AAA Client, page 4-16.

**Step 4** To save your changes and apply them immediately, click **Submit + Restart**.

**Tip** To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

**Note** Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter.



Downloaded from www.Manualslib.com manuals search engine

# Deleting a AAA Client

To delete a AAA client, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the AAA client hostname in the AAA Clients table.
- To delete a AAA client when you have not enabled NDGs, click the AAA client hostname in the AAA Clients table.

The AAA Client Setup for the *Name* page appears.

**Step 3** To delete the AAA client and have the deletion take effect immediately, click **Delete + Restart**.

**Note** Restarting Cisco Secure ACS services clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. As an alternative to restarting when you delete a AAA client, you can click **Delete**. However, when you do this, the change does not take effect until you restart the system, which you can do by clicking **System Configuration**, clicking **Service Control**, and then clicking **Restart**.

A confirmation dialog box appears.

**Step 4** Click **OK**.

Cisco Secure ACS restarts AAA services and the AAA client is deleted.

# AAA Server Configuration

This section presents procedures for configuring AAA servers in the Cisco Secure ACS HTML interface. For additional information about AAA servers, see AAA Servers in Distributed Systems, page 4-3.



Downloaded from www.Manualslib.com manuals search engine

To configure distributed system features for a given Cisco Secure ACS, you must first define the other AAA server(s). For example, all Cisco Secure ACSes involved in replication, remote logging, authentication proxying, and RDBMS synchronization must have AAA server configurations for each other; otherwise, incoming communication from an unknown Cisco Secure ACS is ignored and the distributed system feature will fail.

**Tip** If the AAA Servers table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Distributed System Settings** check box.

This section contains the following topics:


- AAA Server Configuration Options, page 4-22
- Adding a AAA Server, page 4-24
- Editing a AAA Server, page 4-26
- Deleting a AAA Server, page 4-28


# AAA Server Configuration Options

A AAA server configuration enables Cisco Secure ACS to interact with the AAA server that the configuration represents. A AAA server that does not have a corresponding configuration in Cisco Secure ACS, or whose configuration in Cisco Secure ACS is incorrect, does not receive AAA services from Cisco Secure ACS, such as proxied authentication requests, database replication communication, remote logging, and RDBMS synchronization. Also, several distributed systems features require that the other Cisco Secure ACSes included in the distributed system be represented in the AAA Servers table. For more information about distributed systems features, see About Distributed Systems, page 4-2.

The Add AAA Server and AAA Server Setup pages include the following options:

- **AAA Server Name**—The name you assign to the AAA server configuration. The AAA server hostname that is configured in Cisco Secure ACS does not have to match the hostname configured on a network device. We recommend that you adopt a descriptive, consistent naming convention for AAA server names. Maximum length for a AAA server name is 32 characters.



Downloaded from www.Manualslib.com manuals search engine

**Note** After you submit the AAA server name, you cannot change it. If you want to use a different name for a AAA server, delete the AAA server configuration and create a AAA server configuration using the new name.

- **AAA Server IP Address**—The IP address of the AAA server, in dotted, four octet format. For example, 10.77.234.3.
- **Key**—The shared secret of the AAA server. Maximum length for a AAA server key is 32 characters.

  For correct operation, the key must be identical on the remote AAA server and Cisco Secure ACS. Keys are case sensitive. Because shared secrets are not synchronized, it is easy to make mistakes when entering them upon remote AAA servers and Cisco Secure ACS. If the shared secret does not match, Cisco Secure ACS discards all packets from the remote AAA server.
- **Network Device Group**—The name of the NDG to which this AAA server should belong. To make the AAA server independent of NDGs, use the Not Assigned selection.

**Note** This option does not appear if you have not configured Cisco Secure ACS to use NDGs. To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

- **Log Update/Watchdog Packets from this remote AAA Server**—Enables logging of update, or watchdog, packets from AAA clients that are forwarded by the remote AAA server to this Cisco Secure ACS. Watchdog packets are interim packets sent periodically during a session. They provide you with an approximate session length if a AAA client fails and, therefore, no stop packet is received to mark the end of the session.
- **AAA Server Type**—One of the following three types:
  - **RADIUS**—Select this option if the remote AAA server is configured using any type of RADIUS protocol.
  - **TACACS+**—Select this option if the remote AAA server is configured using the TACACS+ protocol.



Downloaded from www.Manualslib.com manuals search engine

  - **Cisco Secure ACS**—Select this option if the remote AAA server is another Cisco Secure ACS. This enables you to configure features that are only available with other Cisco Secure ACSes, such as CiscoSecure user database replication and remote logging.

**Note** The remote Cisco Secure ACS must be using version 2.1 or later.

- **Traffic Type**—The Traffic Type list defines the direction in which traffic to and from the remote AAA server is permitted to flow from this Cisco Secure ACS. The list includes the following options:
  - **Inbound**—The remote AAA server accepts requests that have been forwarded to it and does not forward the requests to another AAA server. Select this option if you do not want to permit any authentication requests to be forwarded from the remote AAA server.
  - **Outbound**—The remote AAA server sends out authentication requests but does not receive them. If a Proxy Distribution Table entry is configured to proxy authentication requests to a AAA server that is configured for Outbound, the authentication request is not sent.
  - **Inbound/Outbound**—The remote AAA server forwards and accepts authentication requests. This allows the selected server to handle authentication requests in any manner defined in the distribution tables.

# Adding a AAA Server

### Before You Begin

For descriptions of the options available while adding a remote AAA server configuration, see AAA Server Configuration Options, page 4-22.

For Cisco Secure ACS to provide AAA services to a remote AAA server, you must ensure that gateway devices between the remote AAA server and Cisco Secure ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports used by AAA protocols, see AAA Protocols—TACACS+ and RADIUS, page 1-6.



Downloaded from www.Manualslib.com manuals search engine

To add and configure a AAA server, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA server is to be assigned. Then, click **Add Entry** below the [name] AAA Servers table.
- To add a AAA server when you have not enabled NDGs, below the AAA Servers table, click **Add Entry**.

The Add AAA Server page appears.

**Step 3** In the AAA Server Name box, type a name for the remote AAA server (up to 32 characters).

**Step 4** In the AAA Server IP Address box, type the IP address assigned to the remote AAA server.

**Step 5** In the Key box, type the shared secret that the remote AAA server and the Cisco Secure ACS use to encrypt the data (up to 32 characters).

**Note** The key is case sensitive. If the shared secret does not match, Cisco Secure ACS discards all packets from the remote AAA server.

**Step 6** From the Network Device Group list, select the NDG to which this AAA server belongs.

**Note** To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then click **Network Device Groups**.

**Step 7** To enable watchdog packets, select the **Log Update/Watchdog Packets from this remote AAA Server** check box.

**Step 8** From the AAA Server Type list, select the AAA server type applicable to the remote AAA server. If the remote AAA server is another Cisco Secure ACS, identify it as such by selecting **CiscoSecure ACS**.



Downloaded from www.Manualslib.com manuals search engine

**Step 9** From the Traffic Type list, select the type of traffic you want to permit between the remote AAA server and Cisco Secure ACS.

**Step 10** To save your changes and apply them immediately, click **Submit + Restart**.

**Tip** To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

**Note** Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter and resets it to zero.

# Editing a AAA Server

Use this procedure to edit the settings for a AAA server that you have previously configured.

**Note** You cannot edit the name of a AAA server. To rename a AAA server, you must delete the existing AAA server entry and then add a new server entry with the new name.

### Before You Begin

For descriptions of the options available while editing a remote AAA server entry, see AAA Server Configuration Options, page 4-22.

For Cisco Secure ACS to provide AAA services to a remote AAA server, you must ensure that gateway devices between the remote AAA server and Cisco Secure ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports used by AAA protocols, see AAA Protocols—TACACS+ and RADIUS, page 1-6.



Downloaded from www.Manualslib.com manuals search engine

To edit a AAA server, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA server is assigned. Then, in the AAA Servers table, click the name of the AAA server to be edited.
- If you have not enabled NDGs, in the AAA Servers table, click the name of the AAA server to be edited.

The AAA Server Setup for *X* page appears.

**Step 3** Enter or select new settings for one or more of the following fields:

- AAA Server IP Address
- Key
- Log Update/Watchdog Packets from this remote AAA Server
- AAA Server Type
- Traffic Type

**Step 4** To save your changes and apply them immediately, click **Submit + Restart**.

**Tip** To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

**Note** Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter and resets it to zero.



Downloaded from www.Manualslib.com manuals search engine

# Deleting a AAA Server

To delete a AAA server, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA server is assigned. Then, click the AAA server name in the AAA Servers table.
- If you have not enabled NDGs, click the AAA server name in the AAA Servers table.

The AAA Server Setup for *X* page appears.

**Step 3** To delete the AAA server and have the deletion take effect immediately, click **Delete + Restart**.

**Note** Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. As an alternative to restarting when you delete a AAA server, in the preceding step you can click **Delete**. However, when you do this, the change does not take effect until you restart the system, which you can do by clicking **System Configuration**, clicking **Service Control**, and then clicking **Restart**.

A confirmation dialog box appears.

**Step 4** Click **OK**.

Cisco Secure ACS performs a restart and the AAA server is deleted.

# Network Device Group Configuration

Network Device Grouping is an advanced feature that enables you to view and administer a collection of network devices as a single logical group. To simplify administration, you can assign each group a name that can be used to refer to all devices within that group. This creates two levels of network devices within



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS—single discrete devices such as an individual router or network access server, and an NDG; that is, a collection of routers or AAA servers.

**Caution** To see the Network Device Groups table in the HTML interface, you must have the Network Device Groups option selected on the Advanced Options page of the Interface Configuration section. Unlike in other areas of Interface Configuration, it is possible to remove from sight an active NDG if you deselect the Network Device Groups option. Therefore, if you choose to configure NDGs, make sure you leave the Network Device Groups option selected on the Advanced Option page.

This section contains the following topics:


- Adding a Network Device Group, page 4-29
- Assigning an Unassigned AAA Client or AAA Server to an NDG, page 4-30
- Reassigning a AAA Client or AAA Server to an NDG, page 4-31
- Renaming a Network Device Group, page 4-32
- Deleting a Network Device Group, page 4-32


# Adding a Network Device Group

You can assign users or groups of users to NDGs. For more information, see one of the following sections:


- Setting TACACS+ Enable Password Options for a User, page 7-35
- Setting Enable Privilege Options for a User Group, page 6-19


To add an NDG, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** Under the Network Device Groups table, click **Add Entry**.



Downloaded from www.Manualslib.com manuals search engine

**Tip** If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select **Network Device Groups**.

**Step 3** In the Network Device Group Name box, type the name of the new NDG.

**Tip** The maximum name length is 24 characters. Quotation marks (“) and commas (,) are not allowed. Spaces are allowed.

**Step 4** Click **Submit**.

The Network Device Groups table displays the new NDG.

**Step 5** To populate the newly established NDG with AAA clients or AAA servers, perform one or more of the following procedures, as applicable:

- Adding a AAA Client, page 4-16
- Adding a AAA Server, page 4-24
- Assigning an Unassigned AAA Client or AAA Server to an NDG, page 4-30
- Reassigning a AAA Client or AAA Server to an NDG, page 4-31

# Assigning an Unassigned AAA Client or AAA Server to an NDG

You use this procedure to assign an unassigned AAA client or AAA server to an NDG. Before you begin this procedure, you should have already configured the client or server and it should appear in the Not Assigned AAA Clients or Not Assigned AAA Servers table.

To assign a network device to an NDG, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** In the Network Device Groups table, click **Not Assigned**.



Downloaded from www.Manualslib.com manuals search engine

**Tip** If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

**Step 3** Click the name of the network device you want to assign to an NDG.

**Step 4** From the Network Device Groups list, select the NDG to which you want to assign the AAA client or AAA server.

**Step 5** Click **Submit**.

The client or server is assigned to an NDG.

# Reassigning a AAA Client or AAA Server to an NDG

To reassign a AAA client or AAA server to a new NDG, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** In the Network Device Groups table, click the name of the current group of the network device.

**Step 3** In either the AAA Clients table or AAA Servers table, as applicable, click the name of the client or server you want to assign to a new NDG.

**Step 4** From the Network Device Group list, select the NDG to which you want to reassign the network device.

**Step 5** Click **Submit**.

The network device is assigned to the NDG you selected.



Downloaded from www.Manualslib.com manuals search engine

# Renaming a Network Device Group

**Caution** When renaming an NDG, ensure that there are no NARs or other shared profile components (SPCs) that invoke the original NDG name. Cisco Secure ACS performs no automatic checking to determine whether the original NDG is still invoked. If a user's authentication request incorporates an SPC that invokes a non-existent (or renamed) NDG, the attempt will fail and the user will be rejected.

To rename an NDG, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** In the Network Device Groups table, click the NDG that you want to rename.

**Tip** If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

**Step 3** At the bottom of the page, click **Rename**.

The Rename Network Device Group page appears.

**Step 4** In the Network Device Group Name box, type the new name (up to 24 characters).

**Step 5** Click **Submit**.

The name of the NDG is changed.

# Deleting a Network Device Group

When you delete an NDG, all AAA clients and AAA servers that belong to the deleted group appear in the Not Assigned AAA Clients or Not Assigned AAA Servers table.



Downloaded from www.Manualslib.com manuals search engine

**Tip** It may be useful to empty an NDG of AAA clients and AAA servers before you delete it. You can do this manually by performing the procedure Reassigning a AAA Client or AAA Server to an NDG, page 4-31, or, in cases where there are a large number of devices to reassign, you can use the RDBMS Synchronization feature.

**Caution** When deleting an NDG, ensure that there are no NARs or other SPCs that invoke the original NDG. Cisco Secure ACS performs no automatic checking to determine whether the original NDG is still invoked. If a user authentication request incorporates an SPC that invokes a non-existent (or renamed) NDG, the attempt will fail and the user will be rejected.

To delete an NDG, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** In the Network Device Groups table, click the NDG that you want to delete.

**Tip** If the Network Device Groups table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

**Step 3** At the bottom of the page, click **Delete Group**.

A confirmation dialog box appears.

**Step 4** Click **OK**.

The NDG is deleted and its name is removed from the Network Device Groups table. Any AAA clients and AAA servers that were in the NDG are now in the Not Assigned AAA Clients or Not Assigned AAA Servers table.



Downloaded from www.Manualslib.com manuals search engine

# Proxy Distribution Table Configuration

This section describes the Proxy Distribution Table and provides procedures for working with the Proxy Distribution Table.

This section contains the following topics:


- About the Proxy Distribution Table, page 4-34
- Adding a New Proxy Distribution Table Entry, page 4-35
- Sorting the Character String Match Order of Distribution Entries, page 4-36
- Editing a Proxy Distribution Table Entry, page 4-37
- Deleting a Proxy Distribution Table Entry, page 4-38


## About the Proxy Distribution Table

If you have Distributed Systems Settings enabled, when you click Network Configuration, you will see the Proxy Distribution Table.

**Tip** To enable Distributed Systems Settings in the Cisco Secure ACS, click **Interface Configuration**, click **Advanced Options**, and then select the **Distributed System Settings** check box.

The Proxy Distribution Table includes entries that show the character strings on which to proxy, the AAA servers to proxy to, whether to strip the character string, and where to send the accounting information (Local/Remote, Remote, or Local). For more information about the proxy feature, see Proxy in Distributed Systems, page 4-4.

The entries you define and place in the Proxy Distribution Table can be considered turnstiles for each authentication request that Cisco Secure ACS receives from the AAA client. The authentication request is defined in the Proxy Distribution Table according to where it is to be forwarded. If a match to an entry in the Proxy Distribution Table that contains proxy information is found, Cisco Secure ACS forwards the request to the appropriate AAA server.

The Character String column in the Proxy Distribution Table always contains an entry of "(Default)". The "(Default)" entry matches authentication requests received by the local Cisco Secure ACS that do not match any other defined



Downloaded from www.Manualslib.com manuals search engine

character strings. While you cannot change the character string definition for the "(Default)" entry, you can change the distribution of authentication requests matching the "(Default)" entry. At installation, the AAA server associated with the "(Default)" entry is the local Cisco Secure ACS. It can sometimes be easier to define strings that match authentication requests to be processed locally rather than defining strings that match authentication requests to be processed remotely. In such a case, associating the "(Default)" entry with a remote AAA server permits you to configure your Proxy Distribution Table with the more easily written entries.

# Adding a New Proxy Distribution Table Entry

To create a Proxy Distribution Table entry, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** Under the Proxy Distribution Table, click **Add Entry**.

**Note** If the Proxy Distribution Table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Distributed System Settings** check box.

**Step 3** In the Character String box, type the string of characters, including the delimiter to forward on when users dial in to be authenticated. For example, .uk.

**Note** Angle brackets (< and >) cannot be used.

**Step 4** From the Position list, select **Prefix** if the character string you typed appears at the beginning of the username or **Suffix** if the character string appears at the end of the username.

**Step 5** From the Strip list, select **Yes** if the character string you entered is to be stripped off the username, or select **No** if it is to be left intact.

**Step 6** In the AAA Servers column, select the AAA server you want to use for proxy. Click **-->** (right arrow button) to move it to the Forward To column.



Downloaded from www.Manualslib.com manuals search engine

**Tip** You can also select additional AAA servers to use for backup proxy if the prior servers fail. To set the order of AAA servers, in the Forward To column, click the name of the applicable server and click **Up** or **Down** to move it into the position you want.

**Tip** If the AAA server you want to use is not listed, click **Network Configuration**, click **AAA Servers**, click **Add Entry** and complete the applicable information.

**Step 7** From the Send Accounting Information list, select one of the following areas to which to report accounting information:

- **Local**—Keep accounting packets on the local Cisco Secure ACS.
- **Remote**—Send accounting packets to the remote Cisco Secure ACS.
- **Local/Remote**—Keep accounting packets on the local Cisco Secure ACS and send them to the remote Cisco Secure ACS.

**Tip** This information is especially important if you are using the Max Sessions feature to control the number of connections a user is allowed. Max Sessions depends on accounting start and stop records, and where the accounting information is sent determines where the Max Sessions counter is tracked. The Failed Attempts log and the Logged in Users report are also affected by where the accounting records are sent.

**Step 8** When you finish, click **Submit** or **Submit + Restart**.

# Sorting the Character String Match Order of Distribution Entries

You can use this procedure to set the priority by which Cisco Secure ACS searches character string entries in the Proxy Distribution Table when users dial in.

To determine the order by which Cisco Secure ACS searches entries in the Proxy Distribution Table, follow these steps:



Downloaded from www.Manualslib.com manuals search engine

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** Below the Proxy Distribution Table, click **Sort Entries**.

**Tip** Before you sort the entries, you must have configured at least two unique Proxy Distribution Table entries in addition to the (Default) table entry.

**Step 3** Select the character string entry to reorder, and then click **Up** or **Down** to move its position to reflect the search order you want.

**Step 4** When you finish sorting, click **Submit** or **Submit + Restart**.

# Editing a Proxy Distribution Table Entry

To edit a Proxy Distribution Table entry, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** In the Character String column of the Proxy Distribution Table, click the distribution entry you want to edit.

The Edit Proxy Distribution Entry page appears.

**Step 3** Edit the entry as necessary.

**Tip** For information about the parameters that make up a distribution entry, see Adding a New Proxy Distribution Table Entry, page 4-35.

**Step 4** When you finish editing the entry, click **Submit** or **Submit + Restart**.



Downloaded from www.Manualslib.com manuals search engine

# Deleting a Proxy Distribution Table Entry

To delete a Proxy Distribution Table entry, follow these steps:

**Step 1** In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

**Step 2** In the Character String column of the Proxy Distribution Table, click the distribution entry you want to delete.

The Edit Proxy Distribution Entry page appears.

**Step 3** Click **Delete**.

A confirmation dialog box appears.

**Step 4** Click **OK**.

The distribution entry is deleted from the Proxy Distribution Table.



Downloaded from www.Manualslib.com manuals search engine

# Shared Profile Components

This chapter addresses the Cisco Secure ACS for Windows Server features found in the Shared Profile Components section of the HTML interface.

This chapter contains the following topics:


- About Shared Profile Components, page 5-1
- Network Access Filters, page 5-2
- Downloadable IP ACLs, page 5-7
- Network Access Restrictions, page 5-14
- Command Authorization Sets, page 5-25


## About Shared Profile Components

The Shared Profile Components section enables you to develop and name reusable, shared sets of authorization components that may be applied to one or more users or groups of users and referenced by name within their profiles. These include network access filters (NAFs), downloadable IP access control lists (ACLs), network access restrictions (NARs), and command authorization sets.

The Shared Profile Components section addresses the scalability of selective authorization. Shared profile components can be configured once and then applied to many users or groups. Without this ability, flexible and comprehensive authorization could only be accomplished by explicitly configuring the authorization of each user group on each device. Creating and applying these



Downloaded from www.Manualslib.com manuals search engine

named shared profile components (downloadable IP ACLs, NAFs, NARs, and command authorization sets) makes it unnecessary to repeatedly enter long lists of devices or commands when defining network access parameters.

# Network Access Filters

This section describes NAFs and provides instructions for creating and managing them.

This section contains the following topics:


- About Network Access Filters, page 5-2
- Adding a Network Access Filter, page 5-3
- Editing a Network Access Filter, page 5-5
- Deleting a Network Access Filter, page 5-7


## About Network Access Filters

A NAF is a named group of any combination of one or more of the following network elements:

- IP addresses
- AAA clients (network devices)
- Network device groups (NDGs)

Using a NAF to specify a downloadable IP ACL or NAR—based on the AAA clients by which the user may access the network—saves you the effort of listing each AAA client explicitly.

- **NAFs in downloadable IP ACLs**—You can associate a NAF with specific ACL contents. A downloadable IP ACL consists of one or more ACL contents (sets of ACL definitions) that are associated with either a single NAF or, by default, “All-AAA-Clients”. This pairing of ACL content with a NAF permits Cisco Secure ACS to determine which ACL content is downloaded according to the IP address of the AAA client making the access request. For more information on using NAFs in downloadable IP ACLs, see About Downloadable IP ACLs, page 5-8.



Downloaded from www.Manualslib.com manuals search engine

- **NAFs in shared network access restrictions**—An essential part of specifying a shared NAR is listing the AAA clients from which user access is permitted or denied. Rather than list every AAA client that makes up a shared NAR, you can simply list one or more NAFs instead of, or in combination with, individual AAA clients. For more information on using NAFs in shared NARs, see About Network Access Restrictions, page 5-15.

**Tip** Shared NARs can contain NDGs, or NAFs, or both. NAFs can contain one or more NDGs.

You can add a NAF that contains any combination of NDG, network devices (AAA clients), or IP addresses. For these network devices or NDGs to be selectable you must have previously configured them in Cisco Secure ACS.

The network elements that make up a NAF can be arranged in any order. For best performance, place the elements most commonly encountered at the top of the Selected Items list. For example, in a NAF where the majority of users gain network access through the NDG "accounting" but you also grant access to a single technical support AAA client with the IP address 205.205.111.222, you would list the NDG first (higher) in the list of network elements to prevent all NAF members from having to be examined against the specified IP address.

# Adding a Network Access Filter

To add a NAF, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

**Step 2** Click **Network Access Filtering**.

The Network Access Filtering table page appears.

**Tip** If Network Access Filtering does not appear as a selection on the Shared Profile Components page, you must enable it on the Advanced Options page of the Interface Configuration section.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** Click **Add**.

The Network Access Filtering edit page appears.

**Step 4** In the **Name** box, type the name of the new network access filter.

**Note** The name of a NAF can contain up to 31 characters. Spaces are not allowed. Names cannot contain the following 10 characters: [ ] , / — - “ ‘ > <

**Step 5** In the **Description** box, type a description of the new network access filter.

**Step 6** Add network elements to the NAF definition as applicable:

**a.** To include an NDG in the NAF definition, from the Network Device Groups box, select the NDG; then click **-->** (right arrow button) to move it to the Selected Items box.

**b.** To include a AAA client in the NAF definition, from the Network Device Groups box select the applicable NDG and then, from the Network Devices box, select the AAA client you want to include. Finally, click **-->** (right arrow button) to move it to the Selected Items box.

**Tip** If you are using NDGs the AAA clients appear in the Network Devices box only when you have selected the NDG to which they belong. Otherwise, if you are not using NDGs, you can select the AAA client from the Network Devices box with no prior NDG selection.

**c.** To include an IP address in the NAF definition, type the IP address in the IP Address box. Click **-->** (right arrow button) to move it to the Selected Items box.

**Note** You can use the wildcard (*) to designate a range within an IP address.

**Step 7** Ensure that the order of the items is what you want. To change the order of items, in the Selected Items box, click the name of an item and then click **Up** or **Down** to move it to the position you want.



Downloaded from www.Manualslib.com manuals search engine

**Tip** You can also remove an item from the Selected Items box by selecting the item and then clicking **<--** (left arrow button) to remove it from the list.

**Step 8** To save your NAF and apply it immediately, click **Submit + Restart**.

**Tip** To save your NAF and apply it later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

**Note** Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter and resets it to zero.

The Network Access Filtering table page appears and lists the name and description of the new NAF.

# Editing a Network Access Filter

To edit a NAF, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

**Step 2** Click **Network Access Filtering**.

The Network Access Filtering table appears.

**Step 3** In the Name column, click the NAF you want to edit.

The Network Access Filter page appears with information displayed for the selected NAF.

**Step 4** Edit the Name or Description of the NAF, type and delete information, as applicable.



Downloaded from www.Manualslib.com manuals search engine

**Caution** If you change the name of a NAF, you invalidate all existing references to that NAF; this may affect the access of users or groups associated with NARs or downloadable ACLs that use that NAF.

**Step 5** To add a NDG to the NAF definition, from the Network Device Groups box, select the NDG you want to add. Click **-->** (right arrow button) to move it to the Selected Items box.

**Step 6** To add a AAA client in the NAF definition, from the Network Device Groups box select the applicable NDG and then, from the Network Devices box, select the AAA client you want to add. Click **-->** (right arrow button) to move it to the Selected Items box.

**Tip** If you are not using NDGs, you begin by selecting the AAA client from the Network Devices box.

**Step 7** To add an IP address to the NAF definition, in the **IP Address** box, type the IP address you want to add. Click **-->** (right arrow button) to move it to the Selected Items box.

**Step 8** To edit an IP address, select it in the Selected Items box and then click **<--** (left arrow button) to move it to the IP address box. Type the changes to the IP address and then click **-->** (right arrow button) to move it back to the Selected Items box.

**Step 9** To remove an element from the Selected Items box, select the item and then click **<--** (left arrow button) to remove it.

**Step 10** To change the order of items, in the Selected Items box, click the name of an item and then click **Up** or **Down** to move it into the position you want. For more information on arranging the order of NAFs see About Network Access Filters, page 5-2.

**Step 11** To save the changes to your NAF and apply them immediately, click **Submit + Restart**.

**Tip** To save your NAF and apply it later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.



Downloaded from www.Manualslib.com manuals search engine

**Note** Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter and resets it to zero.

Cisco Secure ACS re-enters the NAF with the new information, which takes effect immediately.

## Deleting a Network Access Filter

**Before You Begin**

Before you delete a NAF you should remove its association with any NAR or downloadable IP ACL that uses it. Otherwise, any NAR or downloadable IP ACL that references the deleted NAF will be misconfigured and will produce an error.

To delete a NAF, follow these steps:

**Step 1** In the navigation bar, click **Network Access Filtering**.

The Network Access Filtering table page appears.

**Step 2** Click the Name of the NAF you want to delete.

The Network Access Filtering edit page appears.

**Step 3** Click **Delete** and then click **OK** to confirm.

The Network Access Filtering table page appears with the name and description of the NAF removed from the table.

# Downloadable IP ACLs

This section describes downloadable ACLs and provides detailed instructions for configuring and managing them.



Downloaded from www.Manualslib.com manuals search engine

This section contains the following topics:


- About Downloadable IP ACLs, page 5-8
- Adding a Downloadable IP ACL, page 5-10
- Editing a Downloadable IP ACL, page 5-13
- Deleting a Downloadable IP ACL, page 5-14


# About Downloadable IP ACLs

Downloadable IP ACLs enable you to create sets of ACL definitions that you can apply to many users or user groups. These sets of ACL definitions are called ACL contents. Also, by incorporating NAFs, you can control the ACL contents that are sent to the AAA client from which a user is seeking access. That is, a downloadable IP ACL consists of one or more ACL content definitions, each of which is either associated with a NAF or (by default) associated to all AAA clients. (The NAF controls the applicability of specified ACL contents according to the AAA client's IP address. For more information on NAFs and how they regulate downloadable IP ACLs see About Network Access Filters, page 5-2).

Downloadable IP ACLs operate as follows:

1. When Cisco Secure ACS grants a user access to the network, Cisco Secure ACS determines whether a downloadable IP ACL is assigned to that user or to that user's group.
2. If Cisco Secure ACS locates a downloadable IP ACL assigned to the user or the user's group, it determines whether there is an ACL content entry associated with the AAA client that sent the RADIUS authentication request.
3. Cisco Secure ACS sends as part of the user session RADIUS access-accept packet an attribute specifying the named ACL and the version of the named ACL.
4. If the AAA client responds that it does not have the current version of the ACL in its cache (that is, the ACL is new or has changed), Cisco Secure ACS sends the ACL (new or updated) to the device.

Downloadable IP ACLs are an alternative to configuring ACLs in the RADIUS Cisco cisco-av-pair attribute [26/9/1] of each user or user group. You can create a downloadable IP ACL once, give it a name, and then assign the downloadable IP



Downloaded from www.Manualslib.com manuals search engine

ACL to each applicable user or user group by referencing its name. This is more efficient than configuring the RADIUS Cisco cisco-av-pair attribute for each user or user group.

Further, by employing NAFs you can apply different ACL contents to the same user or group of users according to the AAA client they are using. No additional configuration of the AAA client is necessary after you have configured the AAA client to use downloadable IP ACLs from Cisco Secure ACS. Downloadable ACLs are protected by the backup or replication regimen you have established.

While entering the ACL definitions in the Cisco Secure ACS HTML interface, do not use keyword and name entries; in all other respects, use standard ACL command syntax and semantics for the AAA client on which you intend to apply the downloadable IP ACL. The ACL definitions that you enter into Cisco Secure ACS consist of one or more ACL commands. Each ACL command must be on a separate line.

You can add one or more named ACL contents to a downloadable IP ACL. By default each ACL content applies to all AAA clients; however, if you have defined NAFs, you can limit the applicability of each ACL content to the AAA clients listed in the NAF you associate to it. That is, by employing NAFs you can make each ACL content, within a single downloadable IP ACL, applicable to multiple different network devices or network device groups in accordance with your network security strategy. For more information on NAFs, see About Network Access Filters, page 5-2.

Also, you can change the order of the ACL contents listed within a downloadable IP ACL. Cisco Secure ACS examines ACL contents starting from the top of the table and downloads the *first* ACL content it finds with a NAF that includes the AAA client that is being used. In setting the order you should seek to ensure system efficiency by arranging the most widely applicable ACL contents higher on the list; but also realize that if your NAFs include overlapping populations of AAA clients you must proceed from the more specific to the more general. For example, Cisco Secure ACS will download any ACL contents with the "All-AAA-Clients" NAF setting and not consider any that are lower on the list.

To use a downloadable IP ACL on a particular AAA client, the following requirements must be met:

- The AAA client must use RADIUS for authentication.
- The AAA client must support downloadable IP ACLs.



Downloaded from www.Manualslib.com manuals search engine

Examples of Cisco devices that support downloadable IP ACLs are:

- PIX Firewalls
- VPN 3000-series concentrators
- Cisco devices running IOS version 12.3(8)T or greater

An example of the format you should use to enter PIX Firewall ACLs in the ACL Definitions box follows:

```
permit tcp any host 10.0.0.254
permit udp any host 10.0.0.254
permit icmp any host 10.0.0.254
permit tcp any host 10.0.0.253
```

An example of the format you should use to enter VPN 3000 ACLs in the ACL Definitions box follows:

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

For detailed ACL definition information, see the command reference section of your device configuration guide.

# Adding a Downloadable IP ACL

### Before You Begin

You should have already configured any NAFS that you intend to use in your downloadable IP ACL.



Downloaded from www.Manualslib.com manuals search engine

To add a downloadable IP ACL, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

**Step 2** Click **Downloadable IP ACLs**.

**Tip** If Downloadable IP ACLs does not appear on the Shared Profile Components page, you must enable either the User-Level Downloadable ACLs or Group-Level Downloadable ACLs option, or both, on the Advanced Options page of the Interface Configuration section.

**Step 3** Click **Add**.

The Downloadable IP ACLs page appears.

**Step 4** In the Name box, type the name of the new IP ACL.

**Note** The name of an IP ACL may contain up to 27 characters. The name *must not* contain spaces nor any of the following characters:
- [ ] / \ " < > —

**Step 5** In the **Description** box, type a description of the new IP ACL.

**Step 6** To add an ACL content to the new IP ACL, click **Add**.

**Step 7** In the **Name** box, type the name of the new ACL content.

**Note** The name of an ACL content may contain up to 27 characters. The name *must not* contain spaces nor any of the following characters:
- [ ] / \ " < > —

**Step 8** In the **ACL Definitions** box, type the new ACL definition.

**Tip** In entering ACL definitions in the Cisco Secure ACS HTML interface, you do not use keyword and name entries; rather, you begin with a permit/deny keyword. For an example of the proper format of the ACL definitions, see About Downloadable IP ACLs, page 5-8.



Downloaded from www.Manualslib.com manuals search engine

**Step 9** To save the ACL content, click **Submit**.

The Downloadable IP ACLs page appears with the new ACL content listed by name in the ACL Contents column.

**Step 10** To associate a NAF to the ACL content, select a NAF from the Network Access Filtering box to the right of the new ACL content. For information on adding a NAF see Adding a Network Access Filter, page 5-3.

**Note** If you do not assign a NAF, Cisco Secure ACS associates the ACL content to all network devices, which is the default.

**Step 11** Repeat Step 3 through Step 10 until you have completely specified the new IP ACL.

**Step 12** To set the order of the ACL contents, select the radio button for an ACL definition and then click **Up** or **Down** to reposition it in the list.

**Tip** The order of ACL contents is significant. Working from top to bottom, Cisco Secure ACS downloads only the *first* ACL definition that has an applicable NAF setting (including the All-AAA-Clients default setting if used). Typically your list of ACL contents will proceed from the one with the most specific (narrowest) NAF to the one with the most general (All-AAA-Clients) NAF.

**Step 13** To save the IP ACL, click **Submit**.

Cisco Secure ACS enters the new IP ACL, which takes effect immediately. For example, if the IP ACL is for use with PIX Firewalls, it is available to be sent to any PIX Firewall that is attempting authentication of a user who has that downloadable IP ACL assigned to his or her user or group profile. For information on assigning a downloadable IP ACL to user or a user group, see Assigning a Downloadable IP ACL to a User, page 7-21, or Assigning a Downloadable IP ACL to a Group, page 6-30.



Downloaded from www.Manualslib.com manuals search engine

# Editing a Downloadable IP ACL

**Before You Begin**

You should have already configured any NAFs that you intend to use in your editing of the downloadable IP ACL.

To edit a downloadable IP ACL, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

**Step 2** Click **Downloadable IP ACLs**.

The Downloadable IP ACLs table appears.

**Step 3** In the **Name** column, click the IP ACL you want to edit.

The Downloadable IP ACLs page appears with information displayed for the selected ACL.

**Step 4** Edit the Name or Description information, as applicable.

**Step 5** To edit ACL content, click on the ACL Contents entry you want to change.

The Downloadable IP ACL Content page appears.

**Step 6** Edit the Name or ACL Definitions, as applicable.

**Tip** Do not use keyword and name entries in the ACL Definitions box; instead, begin with a permit/deny keyword. For an example of the proper format of the ACL definitions, see About Downloadable IP ACLs, page 5-8.

**Step 7** To save the edited ACL definition, click **Submit**.

**Step 8** To change the NAF associated with an ACL content, select a new NAF setting from the corresponding Network Access Filtering box. You can change as many of the NAF associations in a downloadable IP ACL as you like. For more information on NAFs see About Network Access Filters, page 5-2.

**Step 9** Repeat Step 3 through Step 8 until you are finished.

**Step 10** To change the order of the ACL contents, select the radio button for an ACL definition and then click **Up** or **Down** to reposition it in the list.

**Step 11** To save the edited IP ACL, click **Submit**.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS saves the IP ACL with the new information, which takes effect immediately.

## Deleting a Downloadable IP ACL

**Before You Begin**

You should remove the association of a IP ACL with any user or user group profile before deleting the IP ACL.

To delete an IP ACL, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

**Step 2** Click **Downloadable IP ACLs**.

**Step 3** Click the name of the downloadable IP ACL you want to delete.

The Downloadable IP ACLs page appears with information displayed for the selected IP ACL.

**Step 4** At the bottom of the page, click **Delete**.

A dialog box warns you that you are about to delete an IP ACL.

**Step 5** To confirm that you want to delete the IP ACL, click **OK**.

The selected IP ACL is deleted.

# Network Access Restrictions

This section describes network access restrictions (NARs) and provides detailed instructions for configuring and managing shared NARs.



Downloaded from www.Manualslib.com manuals search engine

This section contains the following topics:


- About Network Access Restrictions, page 5-15
- Adding a Shared Network Access Restriction, page 5-19
- Editing a Shared Network Access Restriction, page 5-23
- Deleting a Shared Network Access Restriction, page 5-24


# About Network Access Restrictions

A NAR is a definition, which you make in Cisco Secure ACS, of additional conditions that must be met before a user can access the network. Cisco Secure ACS applies these conditions using information from attributes sent by your AAA clients. Although there are several ways you can set up NARs, they all are based on matching attribute information sent by a AAA client. Therefore, you must understand the format and content of the attributes your AAA clients send if you want to employ effective NARs.

In setting up a NAR you can choose whether the filter operates positively or negatively. That is, in the NAR you specify whether to permit or deny network access, based on comparison of information sent from AAA clients to the information stored in the NAR. However, if a NAR does not encounter sufficient information to operate, it defaults to denied access. This is shown in Table 5-1.

*Table 5-1 NAR Permit/Deny Conditions*

| | IP-Based | Non-IP Based | Insufficient Information |
|---|---|---|---|
| **Permit** | Access Granted | Access Denied | Access Denied |
| **Deny** | Access Denied | Access Granted | Access Denied |

Cisco Secure ACS supports two types of NAR filters:

- **IP-based filters**—IP-based NAR filters limit access based upon the IP addresses of the end-user client and the AAA client. For more information on this type of NAR filter, see About IP-based NAR Filters, page 5-17.
- **Non-IP-based filters**—Non-IP-based NAR filters limit access based upon simple string comparison of a value sent from the AAA client. The value may be the calling line ID (CLI) number, the Dialed Number Identification Service (DNIS) number, the MAC address, or other value originating from



Downloaded from www.Manualslib.com manuals search engine

the client. For this type of NAR to operate, the value in the NAR description must exactly match what is being sent from the client, including whatever format is used. For example, (217) 555-4534 does not match 217-555-4534. For more information on this type of NAR filter, see About Non-IP-based NAR Filters, page 5-18.

You can define a NAR for, and apply it to, a specific user or user group. For more information on this, see Setting Network Access Restrictions for a User, page 7-11, or Setting Network Access Restrictions for a User Group, page 6-8. However, in the Shared Profile Components section of Cisco Secure ACS you can create and name a *shared* NAR without directly citing any user or user group. You give the shared NAR a name that can be referenced in other parts of the Cisco Secure ACS HTML interface. Then, when you set up users or user groups, you can select none, one, or multiple shared restrictions to be applied. When you specify the application of multiple shared NARs to a user or user group, you choose one of two access criteria: either “All selected filters must permit”, or “Any one selected filter must permit”.

It is important to understand the order of precedence related to the different types of NARs. The order of NAR filtering is as follows:

1. Shared NAR at the user level
2. Shared NAR at the group level
3. Non-shared NAR at the user level
4. Non-shared NAR at the group level

You should also note that denial of access at *any* level takes precedence over settings at another level that do not deny access. This is the one exception in Cisco Secure ACS to the rule that user-level settings override group-level settings. For example, a particular user may have no NAR restrictions at the user level that apply, but if that user belongs to a group that is restricted by either a shared or non-shared NAR, the user is denied access.

Shared NARs are kept in the CiscoSecure user database. You can use the Cisco Secure ACS backup and restore features to back up and restore them. You can also replicate the shared NARs, along with other configurations, to secondary Cisco Secure ACSes.



Downloaded from www.Manualslib.com manuals search engine

## About IP-based NAR Filters

For IP-based NAR filters, ACS uses the following attributes, depending upon the AAA protocol of the authentication request:

- **If you are using TACACS+**—The `rem_addr` field from the TACACS+ start packet body is used.

  **Note** When an authentication request is forwarded by proxy to a Cisco Secure ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

- **If you are using RADIUS IETF**—The `calling-station-id` (attribute 31) and `called-station-id` (attribute 30) fields are used.

AAA clients that do not provide sufficient IP address information (for example, some types of firewall) do not support full NAR functionality.

Other attributes for **IP-based** restrictions, per protocol, include the following NAR fields:

- **If you are using TACACS+**—The NAR fields listed in Cisco Secure ACS use the following values:
  - **AAA client**—The `NAS-IP-address` is taken from the source address in the socket between Cisco Secure ACS and the TACACS+ client.
  - **Port**—The `port` field is taken from the TACACS+ start packet body.
- **If you are using RADIUS**—The NAR fields listed in Cisco Secure ACS use the following values:
  - **AAA client**—The `NAS-IP-address` (attribute 4) or, if NAS-IP-address does not exist, `NAS-identifier` (attribute 32) is used.
  - **Port**—The `NAS-port` (attribute 5) or, if NAS-port does not exist, `NAS-port-ID` (attribute 87) is used.



Downloaded from www.Manualslib.com manuals search engine

## About Non-IP-based NAR Filters

A non-IP-based NAR filter (that is, a **DNIS/CLI-based NAR** filter) is a list of permitted or denied "calling"/"point of access" locations that you can use in restricting a AAA client when you do not have an established IP-based connection. The non-IP-based NAR feature generally uses the calling line ID (CLI) number and the Dialed Number Identification Service (DNIS) number.

However, by entering an IP address in place of the CLI you can use the non-IP-based filter even when the AAA client does not use a Cisco IOS release that supports CLI or DNIS. In another exception to entering a CLI, you can enter a MAC address to permit or deny; for example, when you are using a Cisco Aironet AAA client. Likewise, you could enter the Cisco Aironet AP MAC address in place of the DNIS. The format of what you specify in the CLI box—CLI, IP address, or MAC address—must match the format of what you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

Attributes for **DNIS/CLI-based** restrictions, per protocol, include the following NAR fields:

- **If you are using TACACS+**—The NAR fields listed employ the following values:
  - **AAA client**—The `NAS-IP-address` is taken from the source address in the socket between Cisco Secure ACS and the TACACS+ client.
  - **Port**—The `port` field in the TACACS+ start packet body is used.
  - **CLI**—The `rem-addr` field in the TACACS+ start packet body is used.
  - **DNIS**—The `rem-addr` field taken from the TACACS+ start packet body is used. In cases in which the `rem-addr` data begins with "/" the DNIS field contains the `rem-addr` data without the "/" character.

**Note** When an authentication request is forwarded by proxy to a Cisco Secure ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.



Downloaded from www.Manualslib.com manuals search engine

- **If you are using RADIUS**—The NAR fields listed use the following values:
  - **AAA client**—The `NAS-IP-address` (attribute 4) or, if NAS-IP-address does not exist, `NAS-identifier` (RADIUS attribute 32) is used.
  - **Port**—The `NAS-port` (attribute 5) or, if NAS-port does not exist, `NAS-port-ID` (attribute 87) is used.
  - **CLI**—The `calling-station-ID` (attribute 31) is used.
  - **DNIS**—The `called-station-ID` (attribute 30) is used.

When specifying a NAR you can use asterisks (*) as wildcards for any value, or as part of any value to establish a range. All the values/conditions in a NAR description must be met for the NAR to restrict access; that is, the values are "ANDed".

# Adding a Shared Network Access Restriction

You can create a shared NAR that contains many access restrictions. Although the Cisco Secure ACS HTML interface does not enforce limits to the number of access restrictions in a shared NAR or to the length of each access restriction, there are limits that you must adhere to, as follows:

- The combination of fields for each line item cannot exceed 1024 characters.
- The shared NAR cannot have more than 16 KB of characters. The number of line items supported depends on the length of each line item. For example, if you create a CLI/DNIS-based NAR where the AAA client names are 10 characters, the port numbers are 5 characters, the CLI entries are 15 characters, and the DNIS entries are 20 characters, you can add 450 line items before reaching the 16 KB limit.

**Before You Begin**

Before defining a NAR, you should be sure that you have established the elements you intend to use in that NAR. This means that you must have specified all NAFs and NDGs, and defined all relevant AAA clients, before making them part of the NAR definition. For more information see About Network Access Restrictions, page 5-15.



Downloaded from www.Manualslib.com manuals search engine

To add a shared NAR, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

**Step 2** Click **Network Access Restrictions**.

**Step 3** Click **Add**.

The Network Access Restriction page appears.

**Step 4** In the **Name** box, type a name for the new shared NAR.

**Note** The name can contain up to 31 characters. Leading and trailing spaces are not allowed. Names cannot contain the following four characters: [ ] , /

**Step 5** In the **Description** box, type a description of the new shared NAR.

**Step 6** If you want to permit or deny access based on IP addressing, follow these steps:

a. Select the **Define IP-based access descriptions** check box.

b. To specify whether you are listing addresses that are permitted or denied, from the Table Defines list, select the applicable value.

c. Select or type the applicable information in each of the following boxes:

- **AAA Client**—Select **All AAA clients**, or the name of the NDG, or the NAF, or the individual AAA client, to which access is permitted or denied.
- **Port**—Type the number of the port that you want to permit or deny access to. You can use the wildcard asterisk (*) to permit or deny access to all ports on the selected AAA client.
- **Src IP Address**—Type the IP address to filter on when performing access restrictions. You can use the wildcard asterisk (*) to specify all IP addresses.



Downloaded from www.Manualslib.com manuals search engine

**Note** The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.

d. Click **enter**.

The AAA client, port, and address information appears as a line item in the table.

e. To enter additional IP-based line items, repeat c. and d..

**Step 7** If you want to permit or deny access based on calling location or values other than IP addresses, follow these steps:

a. Select the **Define CLI/DNIS based access restrictions** check box.

b. To specify whether you are listing locations that are permitted or denied, from the Table Defines list, select the applicable value.

c. To specify the clients that this NAR applies to, select one of the following values from the AAA Client list:

- The name of the NDG
- The name of the NAF
- The name of the particular AAA client
- All AAA clients

**Tip** Only NDGs that you have already configured are listed.



Downloaded from www.Manualslib.com manuals search engine

d. To specify the information that this NAR should filter on, type values in the following boxes, as applicable:

**Tip** You can type an asterisk (*) as a wildcard to specify "all" as a value.

- **Port**—Type the number of the port to filter on.
- **CLI**—Type the CLI number to filter on. You can also use this box to restrict access based on values other than CLIs, such as an IP address or MAC address; for information, see About Network Access Restrictions, page 5-15.
- **DNIS**—Type the number being dialed into to filter on.

**Note** The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.

e. Click **enter**.

The information specifying the NAR line item appears in the table.

f. To enter additional non-IP-based NAR line items, repeat c. through e..

**Step 8** To save the shared NAR definition, click **Submit**.

Cisco Secure ACS saves the shared NAR and lists it in the Network Access Restrictions table.



Downloaded from www.Manualslib.com manuals search engine

# Editing a Shared Network Access Restriction

To edit a shared NAR, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

**Step 2** Click **Network Access Restrictions**.

The Network Access Restrictions table appears.

**Step 3** In the **Name** column, click the shared NAR you want to edit.

The Network Access Restriction page appears with information displayed for the selected NAR.

**Step 4** Edit the Name or Description of the NAR, as applicable.

**Step 5** To edit a line item in the IP-based access restrictions table, follow these steps:

**a.** Double-click the line item that you want to edit.

Information for the line item is removed from the table and written to the boxes below the table.

**b.** Edit the information, as necessary.

**Note** The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although Cisco Secure ACS is capable of accepting more than 1024 characters when you add a NAR, you cannot edit such a NAR and Cisco Secure ACS cannot accurately apply it to users.

**c.** Click **enter**.

The edited information for this line item is written to the IP-based access restrictions table.

**Step 6** To remove a line item from the IP-based access restrictions table, follow these steps:

**a.** Select the line item.

**b.** Below the table, click **remove**.

The line item is removed from the IP-based access restrictions table.



Downloaded from www.Manualslib.com manuals search engine

**Step 7** To edit a line item in the CLI/DNIS access restrictions table, follow these steps:

**a.** Double-click the line item that you want to edit.

Information for the line item is removed from the table and written to the boxes below the table.

**b.** Edit the information, as necessary.

**Note** The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although Cisco Secure ACS is capable of accepting more than 1024 characters when you add a NAR, you cannot edit such a NAR and Cisco Secure ACS cannot accurately apply it to users.

**c.** Click **enter**.

The edited information for this line item is written to the CLI/DNIS access restrictions table.

**Step 8** To remove a line item from the CLI/DNIS access restrictions table, follow these steps:

**a.** Select the line item.

**b.** Below the table, click **remove**.

The line item is removed from the CLI/DNIS access restrictions table.

**Step 9** To save the changes you have made, click **Submit**.

Cisco Secure ACS re-enters the filter with the new information, which takes effect immediately.

# Deleting a Shared Network Access Restriction

### Before You Begin

Ensure that you remove the association of a shared NAR to any user or group before you delete that NAR.



Downloaded from www.Manualslib.com manuals search engine

To delete a shared NAR, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

**Step 2** Click **Network Access Restrictions**.

**Step 3** Click the **Name** of the shared NAR you want to delete.

The Network Access Restriction page appears with information displayed for the selected NAR.

**Step 4** At the bottom of the page, click **Delete**.

A dialog box warns you that you are about to delete a shared NAR.

**Step 5** To confirm that you want to delete the shared NAR, click **OK**.

The selected shared NAR is deleted.

# Command Authorization Sets

This section describes command authorization sets and pattern matching and provides detailed instructions for configuring and managing them.

This section contains the following topics:


- About Command Authorization Sets, page 5-26
  - Command Authorization Sets Description, page 5-26
  - Command Authorization Sets Assignment, page 5-28
  - Case Sensitivity and Command Authorization, page 5-29
  - Arguments and Command Authorization, page 5-29
  - About Pattern Matching, page 5-30
- Adding a Command Authorization Set, page 5-31
- Editing a Command Authorization Set, page 5-33
- Deleting a Command Authorization Set, page 5-35




Downloaded from www.Manualslib.com manuals search engine

# About Command Authorization Sets

This section contains the following topics:


- Command Authorization Sets Description, page 5-26
- Command Authorization Sets Assignment, page 5-28
- Case Sensitivity and Command Authorization, page 5-29
- Arguments and Command Authorization, page 5-29
- About Pattern Matching, page 5-30


## Command Authorization Sets Description

Command authorization sets provide a central mechanism to control the authorization of each command issued on any given network device. This greatly enhances the scalability and manageability of setting authorization restrictions. In Cisco Secure ACS, the default command authorization sets include Shell Command Authorization Sets and PIX Command Authorization Sets. Cisco device-management applications, such as Management Center for Firewalls, can instruct Cisco Secure ACS to support additional command authorization set types.

**Note** PIX Command Authorization Sets require that the TACACS+ command authorization request identify the service as “pixshell”. Verify that this service has been implemented in the version of PIX OS your firewalls use; if not, use Shell Command Authorization Sets to perform command authorization for PIXes.

**Tip** As of PIX OS version 6.3, the pixshell service has not been implemented.



Downloaded from www.Manualslib.com manuals search engine

To offer fine-grained control of device-hosted, administrative Telnet sessions, a network device using TACACS+ can request authorization for each command line before its execution. You can define a set of commands that are either permitted or denied for execution by a particular user on a given device. Cisco Secure ACS has further enhanced this capability as follows:

- **Reusable Named Command Authorization Sets**—Without directly citing any user or user group, you can create a named set of command authorizations. You can define several command authorization sets, each delineating different access profiles. For example, a "Help desk" command authorization set could permit access to high level browsing commands, such as "show run", and deny any configuration commands. An "All network engineers" command authorization set could contain a limited list of permitted commands for any network engineer in the enterprise. A "Local network engineers" command authorization set could permit all commands, including IP address configuration.
- **Fine Configuration Granularity**—You can create associations between named command authorization sets and NDGs. Thus, you can define different access profiles for users depending on which network devices they access. You can associate the same named command authorization set with more than one NDG and use it for more than one user group. Cisco Secure ACS enforces data integrity. Named command authorization sets are kept in the CiscoSecure user database. You can use the Cisco Secure ACS Backup and Restore features to back up and restore them. You can also replicate command authorization sets to secondary Cisco Secure ACSes along with other configuration data.

For command authorization set types that support Cisco device-management applications, the benefits of using command authorization sets are similar. You can enforce authorization of various privileges in a device-management application by applying command authorization sets to Cisco Secure ACS groups that contain users of the device-management application. The Cisco Secure ACS groups can correspond to different roles within the device-management application and you can apply different command authorization sets to each group, as applicable.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS has three sequential stages of command authorization filtering. Each command authorization request is evaluated in the following order:

1. **Command Match:** Cisco Secure ACS determines whether the command being processed matches a command listed in the command authorization set. If no matching command is found, command authorization is determined by the Unmatched Commands setting, which is either permit or deny. Otherwise, if the command is matched, evaluation continues.
2. **Argument Match:** Cisco Secure ACS determines whether the command arguments presented match the command arguments listed in the command authorization set.
   - If any argument is unmatched, command authorization is determined by whether the Permit Unmatched Args option is enabled. If unmatched arguments are permitted, the command is authorized and evaluation ends; otherwise, the command is not authorized and evaluation ends.
   - If all arguments are matched, evaluation continues.
3. **Argument Policy:** Having determined that the arguments in the command being evaluated match the arguments listed in the command authorization set, Cisco Secure ACS determines whether each command argument is explicitly permitted. If all arguments are explicitly permitted, Cisco Secure ACS grants command authorization. If any arguments is not permitted, Cisco Secure ACS denies command authorization.

## Command Authorization Sets Assignment

For information on assigning command authorization sets, see the following procedures:

- **Shell Command Authorization Sets**—See either of the following:
  - Configuring a Shell Command Authorization Set for a User Group, page 6-33
  - Configuring a Shell Command Authorization Set for a User, page 7-26
- **PIX Command Authorization Sets**—See either of the following:
  - Configuring a PIX Command Authorization Set for a User Group, page 6-35
  - Configuring a PIX Command Authorization Set for a User, page 7-29



Downloaded from www.Manualslib.com manuals search engine

- **Device Management Command Authorization Sets**—See either of the following:
  - Configuring Device-Management Command Authorization for a User Group, page 6-37
  - Configuring Device-Management Command Authorization for a User, page 7-30

## Case Sensitivity and Command Authorization

When performing command authorization, Cisco Secure ACS evaluates commands and arguments in a case-sensitive manner. For successful command authorization, you must configure command authorization sets with case-sensitive commands and arguments.

As an additional complication, a device requesting command authorization may send commands and arguments using a case different from the one you typed to issue the command.

For example, if you type the following command during a router-hosted session:

```
interface FASTETHERNET 0/1
```

the router may submit the command and arguments to Cisco Secure ACS as:

```
interface FastEthernet 0 1
```

If, for the **interface** command, the command authorization set explicitly permits the FastEthernet argument using the spelling “fastethernet”, Cisco Secure ACS fails the command authorization request. If the command authorization rule instead permits the argument “FastEthernet”, Cisco Secure ACS grants the command authorization request. The case used in command authorization sets must match what the device sends, which may or may not match the case you use when you type the command.

## Arguments and Command Authorization

When you explicitly permit or deny arguments rather than rely on Cisco Secure ACS to permit unmatched arguments, you must make certain that you know how devices send arguments to Cisco Secure ACS. A device requesting command authorization may send different arguments than the user typed to issue the command.



Downloaded from www.Manualslib.com manuals search engine

For example, if a user typed the following command during a router-hosted session:

```
interface FastEthernet0/1
```

the router may send the command and arguments Cisco Secure ACS as follows:

```
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd=interface
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=FastEthernet
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=0
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=1
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=<cr>
```

In this example, the router sees multiple arguments where the user typed one string of characters without spaces after the command. It also omits the slash character that separated 0 and 1 when the user issued the command.

If the command authorization rule for the **interface** command explicitly permits the FastEthernet argument using the spelling “FastEthernet0/1”, Cisco Secure ACS fails the command authorization request because it does not match what the router submitted to Cisco Secure ACS. If the command authorization rule instead permits the argument “FastEthernet 0 1", Cisco Secure ACS grants the command authorization request. The case of arguments specified in command authorization sets must match what the device sends, which may or may not match the case you use when you type the arguments.

## About Pattern Matching

For permit/deny command arguments, Cisco Secure ACS applies pattern matching. That is, the argument **permit wid** matches any argument that contains the string **wid**. Thus, for example, **permit wid** would allow not only the argument **wid** but also the arguments **anywid** and **widget**.

To limit the extent of pattern matching you can add the following expressions:

- **dollarsign ($)**—Expresses that the argument must end with what has gone before. Thus **permit wid$** would match **wid** or **anywid**, but not **widget**.
- **caret (^)**—Expresses that the argument must begin with what follows. Thus **permit ^wid** would match **wid** or **widget**, but not **anywid**.

You can combine these expressions to specify absolute matching. In the example given, you would use **permit ^wid$** to ensure that only **wid** was permitted, and not **anywid** or **widget**.



Downloaded from www.Manualslib.com manuals search engine

To permit/deny commands that carry no arguments, you can use absolute matching to specify the null argument condition. For example, you use **permit ^$** to permit a command with no arguments. Alternatively, entering **permit <cr>** has the same effect. Either of these methods can be used, with the **Permit Unmatched Args** option unselected, to match and therefore permit or deny commands that have no argument.

# Adding a Command Authorization Set

To add a command authorization set, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page lists the command authorization set types available. These always include Shell Command Authorization Sets and may include others, such as command authorization set types that support Cisco device-management applications.

**Step 2** Click one of the listed command authorization set types, as applicable.

The selected Command Authorization Sets table appears.

**Step 3** Click **Add**.

The applicable Command Authorization Set page appears. Depending upon the type of command authorization set you are adding, the contents of the page vary. Below the Name and Description boxes, Cisco Secure ACS displays either additional boxes or an expandable checklist tree. The expandable checklist tree appears for device command set types that support a Cisco device-management application.

**Step 4** In the Name box, type a name for the command authorization set.

**Note** The set name can contain up to 27 characters. Names cannot contain the following characters:
# ? " * > <
Leading and trailing spaces are not allowed.

**Step 5** In the Description box, type a description of the command authorization set.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** If Cisco Secure ACS displays an expandable checklist tree below the Name and Description boxes, use the checklist tree to specify the actions permitted by the command authorization set. To do so, follow these steps:

**a.** To expand a checklist node, click the plus (+) symbol to its left.

**b.** To enable an action, select its check box. For example, to enable a Device View action, select the **View** check box under the Device checklist node.

**Tip** Selecting an expandable check box node selects all check boxes within that node. Selecting the first check box in the checklist tree selects all check boxes in the checklist tree.

**c.** To enable other actions in this command authorization set, repeat Step a and Step b, as needed.

**Step 7** If Cisco Secure ACS displays additional boxes below the Name and Description boxes, use the boxes to specify the commands and arguments permitted or denied by the command authorization set. To do so, follow these steps:

**a.** To specify how Cisco Secure ACS should handle unmatched commands, select either the **Permit** or **Deny** option, as applicable.

**Note** The default setting is Deny.

**b.** In the box just above the Add Command button, type a command that is to be part of the set.

**Caution** Enter the full command word; if you use command abbreviations, authorization control may not function.

**Note** Enter only the command portion of the command/argument string here. Arguments are added only after the command is listed. For example, with the command/argument string “show run” you would type only the command **show**.



Downloaded from www.Manualslib.com manuals search engine

c. Click **Add Command**.

The typed command is added to the command list box.

d. To add an argument to a command, in the command list box, select the command and then type the argument in the box to the right of the command.

**Note** The correct format for arguments is <permit | deny> <argument>. For example, with the command **show** already listed, you might enter **permit run** as the argument.

**Tip** You can list several arguments for a single command by pressing Enter between arguments.

e. To allow arguments, which you have not listed, to be effective with this command, select the **Permit Unmatched Args** check box.

f. To add other commands to this command authorization set, repeat Step a through Step e.

**Step 8** To save the command authorization set, click **Submit**.

Cisco Secure ACS displays the name and description of the new command authorization set in the applicable Command Authorization Sets table.

# Editing a Command Authorization Set

To edit a command authorization set, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page lists the command authorization set types available.

**Step 2** Click a command authorization set type, as applicable.

The selected Command Authorization Sets table appears.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** From the Name column, click the name of the set you want to change.

Information for the selected set appears on the applicable Command Authorization Set page.

**Step 4** If an expandable checklist tree appears below the Name and Description boxes, you can do any or all of the following:

- To expand a checklist node, click the plus (+) symbol to its left. To collapse an expanded checklist node, click the minus (-) symbol to its left.
- To enable an action, select its check box. For example, to enable a Device View action, select the View check box under the Device checklist node.

**Tip** Selecting an expandable check box node selects all check boxes within that node. Selecting the first check box in the checklist tree selects all check boxes in the checklist tree.

- To disable an action, clear its check box. For example, to disable a Device View action, clear the View check box under the Device checklist node.

**Step 5** If additional boxes appear below the Name and Description boxes, you can do any or all of the following:

- To change the set Name or Description, edit the words in the corresponding box.
- To remove a command from the set, from the Matched Commands list, select the command, and then click **Remove Command**.
- To edit arguments of a command, from the command list box, select the command and then type changes to the arguments in the box to the right of the command list box.

**Step 6** To save the set, click **Submit**.



Downloaded from www.Manualslib.com manuals search engine

# Deleting a Command Authorization Set

To delete a command authorization set, follow these steps:

**Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page lists the command authorization set types available.

**Step 2** Click a command authorization set type, as applicable.

The selected Command Authorization Sets table appears.

**Step 3** From the Name column, click the name of the command set you want to delete.

Information for the selected set appears on the applicable Command Authorization Set page.

**Step 4** Click **Delete**.

A dialog box warns you that you are about to delete a command authorization set.

**Step 5** To confirm that you want to delete that command authorization set, click **OK**.

Cisco Secure ACS displays the applicable Command Authorization Sets table. The command authorization set is no longer listed.



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

# User Group Management

This chapter provides information about setting up and managing user groups in Cisco Secure ACS for Windows Server to control authorization. Cisco Secure ACS enables you to group network users for more efficient administration. Each user can belong to only one group in Cisco Secure ACS. You can establish up to 500 groups to effect different levels of authorization.

Cisco Secure ACS also supports external database group mapping; that is, if your external user database distinguishes user groups, these groups can be mapped into Cisco Secure ACS. And if the external database does not support groups, you can map all users from that database to a Cisco Secure ACS user group. For information about external database mapping, see Chapter 16, “User Group Mapping and Specification”.

Before you configure Group Setup, you should understand how this section functions. Cisco Secure ACS dynamically builds the Group Setup section interface depending on the configuration of your network devices and the security protocols being used. That is, what you see under Group Setup is affected by settings in the Network Configuration and Interface Configuration sections.

This chapter contains the following topics:


- About User Group Setup Features and Functions, page 6-2
- Basic User Group Settings, page 6-3
- Configuration-specific User Group Settings, page 6-16
- Group Setting Management, page 6-54




Downloaded from www.Manualslib.com manuals search engine

# About User Group Setup Features and Functions

The Group Setup section of the Cisco Secure ACS HTML interface is the centralized location for operations regarding user group configuration and administration. For information about network device groups (NDGs), see Network Device Group Configuration, page 4-28.

This section contains the following topics:


- Default Group, page 6-2
- Group TACACS+ Settings, page 6-2


## Default Group

If you have not configured group mapping for an external user database, Cisco Secure ACS assigns users who are authenticated by the Unknown User Policy to the Default Group the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, Cisco Secure ACS retains the group mappings you configured before upgrading.

## Group TACACS+ Settings

Cisco Secure ACS enables a full range of settings for TACACS+ at the group level. If a AAA client has been configured to use TACACS+ as the security control protocol, you can configure standard service protocols, including PPP IP, PPP LCP, ARAP, SLIP, and shell (exec), to be applied for the authorization of each user who belongs to a particular group.

**Note** You can also configure TACACS+ settings at the user level. User-level settings always override group level settings.

Cisco Secure ACS also enables you to enter and configure new TACACS+ services. For information about how to configure a new TACACS+ service to appear on the group setup page, see Protocol Configuration Options for TACACS+, page 3-7.



Downloaded from www.Manualslib.com manuals search engine

If you have configured Cisco Secure ACS to interact with a Cisco device-management application, new TACACS+ services may appear automatically, as needed, to support the device-management application. For more information about Cisco Secure ACS interaction with device-management applications, see Support for Cisco Device-Management Applications, page 1-19.

You can use the Shell Command Authorization Set feature to configure TACACS+ group settings. This feature enables you to apply shell commands to a particular user group in the following ways:

- Assign a shell command authorization set, which you have already configured, for any network device.
- Assign a shell command authorization set, which you have already configured, to particular NDGs.
- Permit or deny specific shell commands, which you define, on a per-group basis.

For more information about shell command authorization sets, see Chapter 5, "Shared Profile Components".

# Basic User Group Settings

This section presents the basic activities you perform when configuring a new user group.

This section contains the following topics:

- Group Disablement, page 6-4
- Enabling VoIP Support for a User Group, page 6-4
- Setting Default Time-of-Day Access for a User Group, page 6-5
- Setting Callback Options for a User Group, page 6-7
- Setting Network Access Restrictions for a User Group, page 6-8
- Setting Max Sessions for a User Group, page 6-12
- Setting Usage Quotas for a User Group, page 6-14



Downloaded from www.Manualslib.com manuals search engine

# Group Disablement

You perform this procedure to disable a user group and, thereby, to prevent any member of the disabled group from authenticating.

**Note** Group Disablement is the only setting in Cisco Secure ACS where the setting at the group level may override the setting at the user level. If group disablement is set, all users within the disabled group are denied authentication, regardless of whether or not the user account is disabled. However, if a user account is disabled it remains disabled regardless of the status of the corresponding user group disablement setting. In other words, when group and user account disablement settings differ, Cisco Secure ACS defaults to preventing network access.

To disable a group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select the group you want to disable, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** In the Group Disabled table, select the check box labeled **This group is disabled - and all users of this group are disabled**.

**Step 4** To disable the group immediately, click **Submit + Restart**.
For more information, see Saving Changes to User Group Settings, page 6-56.

The group is disabled, and all members of the group are disabled.

# Enabling VoIP Support for a User Group

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Voice-over-IP (VoIP) Group Settings** check box.



Downloaded from www.Manualslib.com manuals search engine

Perform this procedure to enable support for the null password function of VoIP. This enables users to authenticate (session or telephone call) on only the user ID (telephone number).

When you enable VoIP at the group level, all users in this group become VoIP users, and the user IDs are treated similarly to a telephone number. VoIP users do not need to enter passwords to authenticate.

**Caution** Enabling VoIP disables password authentication and most advanced settings, including password aging and protocol attributes.

To enable VoIP support for a group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select the group you want to configure for VoIP support, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** In the Voice-over-IP Support table, select the check box labeled **This is a Voice-over-IP (VoIP) group - and all users of this group are VoIP users**.

**Step 4** To save the group settings you have just made, click **Submit**.
For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 5** To continue, and specify other group settings, perform other procedures in this chapter, as applicable.

# Setting Default Time-of-Day Access for a User Group

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Default Time-of-Day / Day-of-Week Specification** check box.



Downloaded from www.Manualslib.com manuals search engine

To define the times during which users in a particular group are permitted or denied access, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** In the Default Time-of-Day Access Settings table, select the **Set as default Access Times** check box.

**Note** You must select the **Set as default Access Times** check box to limit access based on time or day.

Times at which the system permits access are highlighted in green on the day and hour matrix.

**Note** The default sets accessibility during all hours.

**Step 4** In the day and hour matrix, click the times at which you do *not* want to permit access to members of this group.

**Tip** Clicking times of day on the graph deselects those times; clicking again reselects them.
At any time, you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

**Step 5** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Setting Callback Options for a User Group

Callback is a command string that is passed back to the access server. You can use callback strings to initiate a modem to call the user back on a specific number for added security or reversal of line charges. There are three options, as follows:

- **No callback allowed**—Disables callback for users in this group. This is the default setting.
- **Dialup client specifies callback number**—Allows the dialup client to specify the callback number. The dialup client must support RFC 1570, PPP LCP Extensions.
- **Use Windows Database callback settings (where possible)**—Uses the Microsoft Windows callback settings. If a Windows account for a user resides in a remote domain, the domain in which Cisco Secure ACS resides must have a two-way trust with that domain for the Microsoft Windows callback settings to operate for that user.

**Note** The password aging feature does not operate correctly if you also use the callback feature. When callback is used, users cannot receive password aging messages at login.

To set callback options for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** Select a group from the Group list, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** In the Callback table, select one of the following three options:

- No callback allowed
- Dialup client specifies callback number
- Use Windows Database callback settings (where possible)

**Step 4** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Setting Network Access Restrictions for a User Group

The Network Access Restrictions table in Group Setup enables you to apply network access restrictions (NARs) in three distinct ways:

- Apply existing shared NARs by name.
- Define IP-based group access restrictions to permit or deny access to a specified AAA client or to specified ports on a AAA client when an IP connection has been established.
- Define CLI/DNIS-based group NARs to permit or deny access to either, or both, the calling line ID (CLI) number or the Dialed Number Identification Service (DNIS) number used.

**Note** You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see About Network Access Restrictions, page 5-15.

Typically, you define (shared) NARs from within the Shared Components section so that these restrictions can be applied to more than one group or user. For more information, see Adding a Shared Network Access Restriction, page 5-19. You must have enabled the Group-Level Shared Network Access Restriction check box on the Advanced Options page of the Interface Configuration section for these options to appear in the Cisco Secure ACS HTML interface.

However, Cisco Secure ACS also enables you to define and apply a NAR for a single group from within the Group Setup section. You must have enabled the Group-Level Network Access Restriction setting under the Advanced Options page of the Interface Configuration section for single group IP-based filter options and single group CLI/DNIS-based filter options to appear in the Cisco Secure ACS HTML interface.



Downloaded from www.Manualslib.com manuals search engine

**Note** When an authentication request is forwarded by proxy to a Cisco Secure ACS server, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

To set NARs for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** To apply a previously configured shared NAR to this group, follow these steps:

**Note** To apply a shared NAR, you must have configured it under Network Access Restrictions in the Shared Profile Components section. For more information, see Adding a Shared Network Access Restriction, page 5-19.

a. Select the **Only Allow network access when** check box.

b. To specify whether one or all shared NARs must apply for a member of the group to be permitted access, select one of the following options:

- All selected shared NARS result in permit
- Any one selected shared NAR results in permit

c. Select a shared NAR name in the Shared NAR list, and then click **-->** (right arrow button) to move the name into the Selected Shared NARs list.

**Tip** To view the server details of the shared NARs you have selected to apply, you can click either **View IP NAR** or **View CLID/DNIS NAR**, as applicable.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** To define and apply a NAR, for this particular user group, that permits or denies access to this group based on IP address, or IP address and port, follow these steps:

**Tip** You should define most NARs from within the Shared Components section so that the restrictions can be applied to more than one group or user. For more information, see Adding a Shared Network Access Restriction, page 5-19.

a. In the Per Group Defined Network Access Restrictions section of the Network Access Restrictions table, select the **Define IP-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select either **Permitted Calling/Point of Access Locations** or **Denied Calling/Point of Access Locations**.

c. Select or enter the information in the following boxes:

- **AAA Client**—Select either All AAA Clients or the name of the NDG or the name of the individual AAA client to which to permit or deny access.
- **Port**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports on the selected AAA client.
- **Address**—Type the IP address or addresses to filter on when performing access restrictions. You can use the wildcard asterisk (*).

**Note** The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.

d. Click **Enter**.

The specified the AAA client, port, and address information appears in the NAR Access Control list.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** To permit or deny access to this user group based on calling location or values other than an established IP address, follow these steps:

**a.** Select the **Define CLI/DNIS-based access restrictions** check box.

**b.** To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one of the following:

- Permitted Calling/Point of Access Locations
- Denied Calling/Point of Access Locations

**c.** From the AAA Client list, select either All AAA Clients or the name of the NDG or the name of the particular AAA client to which to permit or deny access.

**d.** Complete the following boxes:

**Note** You must type an entry in each box. You can use the wildcard asterisk (*) for all or part of a value. The format you use must match the format of the string you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **PORT**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access based on part of the number or all numbers.

**Tip** This is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet client MAC address. For more information, see About Network Access Restrictions, page 5-15.

- **DNIS**—Type the DNIS number to restrict access based on the number into which the user will be dialing. You can use the wildcard asterisk (*) to permit or deny access based on part of the number or all numbers.

**Tip** This is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet AP MAC address. For more information, see About Network Access Restrictions, page 5-15.



Downloaded from www.Manualslib.com manuals search engine

**Note** The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.

e. Click **Enter**.

The information, specifying the AAA client, port, CLI, and DNIS appears in the list.

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Setting Max Sessions for a User Group

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Max Sessions** check box.

Perform this procedure to define the maximum number of sessions available to a group, or to each user in a group, or both. The settings are as follows:

- **Sessions available to group**—Sets the maximum number of simultaneous connections for the entire group.
- **Sessions available to users of this group**—Sets the maximum number of total simultaneous connections for each user in this group.

**Tip** As an example, Sessions available to group is set to 10 and Sessions available to users of this group is set to 2. If each user is using the maximum 2 simultaneous sessions, no more than 5 users can log in.



Downloaded from www.Manualslib.com manuals search engine

**Note** A session is any type of connection supported by RADIUS or TACACS+, such as PPP, NAS prompt, Telnet, ARAP, IPX/SLIP.

**Note** The default setting for group Max Sessions is Unlimited for both the group and the user within the group.

To configure max sessions settings for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** In the Max Sessions table, under Sessions available to group, select one of the following options:

- **Unlimited**—Select to allow this group an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- *n*—Type the maximum number of simultaneous sessions to allow this group.

**Step 4** In the lower portion of the Max Sessions table, under Sessions available to users of this group, select one of the following two options:

- **Unlimited**—Select to allow each individual in this group an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- *n*—Type the maximum number of simultaneous sessions to allow each user in this group.

**Note** Settings made in User Setup override group settings. For more information, see Setting Max Sessions Options for a User, page 7-16.

**Step 5** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Setting Usage Quotas for a User Group

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Usage Quotas** check box.

Perform this procedure to define usage quotas for members of a group. Session quotas affect each user of a group individually, not the group collectively. You can set quotas for a given period in two ways:

- By total duration of session
- By the total number of sessions

If you make no selections in the Usage Quotas section for a group, no usage quotas are enforced on users assigned to that group, unless you configure usage quotas for the individual users.

**Note** The Usage Quotas section on the Group Settings page does not show usage statistics.
Usage statistics are available only on the settings page for an individual user. For more information, see Setting User Usage Quotas Options, page 7-18.

When a user exceeds his or her assigned quota, Cisco Secure ACS denies that user access upon attempting to start a session. If a quota is exceeded during a session, Cisco Secure ACS allows the session to continue.

You can reset the usage quota counters for all users of a group from the Group Settings page. For more information about resetting usage quota counters for a whole group, see Resetting Usage Quota Counters for a User Group, page 6-55.

**Tip** To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated when the user logs off. If the AAA client through which the user is accessing your



Downloaded from www.Manualslib.com manuals search engine

network fails, the quota is not updated. In the case of multiple sessions, such as with ISDN, the quota is not updated until all sessions terminate. This means that a second channel will be accepted even if the first channel has exhausted the quota for the user.

To set user usage quotas for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** To define usage quotas based on duration of sessions, follow these steps:

**a.** In the Usage Quotas table, select the **Limit each user of this group to** *x* **hours of online time** *per time unit* check box.

**b.** Type the number of hours to which you want to limit group members in the **to** *x* **hours** box.
Use decimal values to indicate minutes. For example, a value of 10.5 would equal ten hours and 30 minutes.

**Note** Up to 5 characters are allowed in the to *x* hours box.

**c.** Select the period for which the quota is effective from the following:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Total**—An ongoing count of hours, with no end.

**Step 4** To define user session quotas based on number of sessions, follow these steps:

**a.** In the Usage Quotas table, select the **Limit each user of this group to** *x* **sessions** check box.

**b.** Type the number of sessions to which you want to limit users in the **to** *x* **sessions** box.



Downloaded from www.Manualslib.com manuals search engine

**Note** Up to 5 characters are allowed in the to *x* sessions box.

c. Select the period for which the session quota is effective from the following:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Total**—An ongoing count of session, with no end.

**Step 5** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Configuration-specific User Group Settings

This section details procedures that you perform only as applicable to your particular network security configuration. For instance, if you have no token server configured, you do not have to set token card settings for each group.

**Note** When a vendor-specific variety of RADIUS is configured for use by network devices, the RADIUS (IETF) attributes are available because they are the base set of attributes, used by all RADIUS vendors per the RADIUS IETF specifications.

The HTML interface content corresponding to these procedures is dynamic, its appearance based upon the following two factors:

- For a particular protocol (RADIUS or TACACS+) to be listed, at least one AAA client entry in the Network Configuration section of the HTML interface must use that protocol. For more information, see AAA Client Configuration, page 4-11.



Downloaded from www.Manualslib.com manuals search engine

- To cause specific protocol attributes to appear on a group profile page, you must enable the display of those attributes in the Interface Configuration section of the HTML interface. For more information, see Protocol Configuration Options for TACACS+, page 3-7, or Protocol Configuration Options for RADIUS, page 3-11.

This section contains the following topics:


- Setting Token Card Settings for a User Group, page 6-18
- Setting Enable Privilege Options for a User Group, page 6-19
- Enabling Password Aging for the CiscoSecure User Database, page 6-21
- Enabling Password Aging for Users in Windows Databases, page 6-26
- Setting IP Address Assignment Method for a User Group, page 6-28
- Assigning a Downloadable IP ACL to a Group, page 6-30
- Configuring TACACS+ Settings for a User Group, page 6-31
- Configuring a Shell Command Authorization Set for a User Group, page 6-33
- Configuring a PIX Command Authorization Set for a User Group, page 6-35
- Configuring Device-Management Command Authorization for a User Group, page 6-37
- Configuring IETF RADIUS Settings for a User Group, page 6-38
- Configuring Cisco IOS/PIX RADIUS Settings for a User Group, page 6-40
- Configuring Cisco Aironet RADIUS Settings for a User Group, page 6-41
- Configuring Ascend RADIUS Settings for a User Group, page 6-43
- Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group, page 6-44
- Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 6-46
- Configuring Microsoft RADIUS Settings for a User Group, page 6-47
- Configuring Nortel RADIUS Settings for a User Group, page 6-49
- Configuring Juniper RADIUS Settings for a User Group, page 6-50
- Configuring BBSM RADIUS Settings for a User Group, page 6-51
- Configuring Custom RADIUS VSA Settings for a User Group, page 6-53




Downloaded from www.Manualslib.com manuals search engine

# Setting Token Card Settings for a User Group

**Note** If this section does not appear, configure a token server. Then, click **External User Databases**, click **Database Configuration**, and then add the applicable token card server.

Perform this procedure to allow a token to be cached. This means users can use a second B channel without having to enter a second one-time password (OTP).

**Caution** This option is for use with token caching only for ISDN terminal adapters. You should fully understand token caching and ISDN concepts and principles before implementing this option. Token caching allows you to connect to multiple B channels without having to provide a token for each channel connection. Token card settings are applied to all users in the selected group.

Options for token caching include the following:

- **Session**—You can select Session to cache the token for the entire session. This allows the second B channel to dynamically go in and out of service.
- **Duration**—You can select Duration and specify a period of time to have the token cached (from the time of first authentication). If this time period expires, the user cannot start a second B channel.
- **Session and Duration**—You can select both Session and Duration so that, if the session runs longer than the duration value, a new token is required to open a second B channel. Type a value high enough to allow the token to be cached for the entire session. If the session runs longer than the duration value, a new token is required to open a second B channel.

To set token card settings for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** From the Jump To list at the top of the page, choose **Token Cards**.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** In the Token Card Settings table, to cache the token for the entire session, select **Session**.

**Step 5** Also in the Token Card Settings table, to cache the token for a specified time period (measured from the time of first authentication), follow these steps:

a. Select **Duration**.

b. Type the duration length in the box.

c. Select the unit of measure, either Seconds, Minutes or Hours.

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Setting Enable Privilege Options for a User Group

**Note** If this section does not appear, click **Interface Configuration** and then click **TACACS+ (Cisco)**. At the bottom of the page in the Advanced Configuration Options table, select the **Advanced TACACS+ features** check box.

Perform this procedure to configure group-level TACACS+ enable parameters. The three possible TACACS+ enable options are as follows:

- **No Enable Privilege**—(default) Select this option to disallow enable privileges for this user group.
- **Max Privilege for Any AAA Client**—Select this option to select the maximum privilege level for this user group for any AAA client on which this group is authorized.
- **Define max Privilege on a per-network device group basis**—Select this option to define maximum privilege levels for an NDG. To use this option, you create a list of device groups and corresponding maximum privilege levels. See your AAA client documentation for information about privilege levels.



Downloaded from www.Manualslib.com manuals search engine

**Note** To define levels in this manner, you must have configured the option in Interface Configuration; if you have not done so already, click **Interface Configuration**, click **Advanced Settings**, and then select the **Network Device Groups** check box.

If you are using NDGs, this option lets you configure the NDG for enable-level mapping rather than having to do it for each user in the group.

To set enable privilege options for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** From the Jump To list at the top of the page, choose **Enable Options**.

**Step 4** Do one of the following:

- To disallow enable privileges for this user group, select the **No Enable Privilege** option.
- To set the maximum privilege level for this user group, for any ACS on which this group is authorized, select the **Max Privilege for Any Access Server** option. Then, select the maximum privilege level from the list.
- To define the maximum NDG privilege level for this user group, select the **Define max Privilege on a per-network device group basis** option. Then, from the lists, select the NDG and a corresponding privilege level. Finally, click **Add Association**.

  **Result:** The association of NDG and maximum privilege level appears in the table.

**Step 5** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Enabling Password Aging for the CiscoSecure User Database

The password aging feature of Cisco Secure ACS enables you to force users to change their passwords under one or more of the following conditions:

- After a specified number of days (age-by-date rules).
- After a specified number of logins (age-by-uses rules).
- The first time a new user logs in (password change rule).

**Varieties of Password Aging Supported by Cisco Secure ACS**

Cisco Secure ACS supports four distinct password aging mechanisms:

- **PEAP and EAP-FAST Windows Password Aging**—Users must be in the Windows user database and be using a Microsoft client that supports EAP, such as Windows XP. For information on the requirements and configuration of this password aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-26.
- **RADIUS-based Windows Password Aging**—Users must be in the Windows user database and be using the Windows Dial-up Networking (DUN) client. For information on the requirements and configuration of this password aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-26.
- **Password Aging for Device-hosted Sessions**—Users must be in the CiscoSecure user database, the AAA client must be running TACACS+, and the connection must use Telnet. You can control the ability of users to change passwords during a device-hosted Telnet session. You can also control whether Cisco Secure ACS propagates passwords changed by this feature. For more information, see Local Password Management, page 8-5.
- **Password Aging for Transit Sessions**—Users must be in the CiscoSecure user database. Users must use a PPP dialup client. Further, the end-user client must have CiscoSecure Authentication Agent (CAA) installed.

**Tip** The CAA software is available at http://www.cisco.com.

Also, to run password aging for transit sessions, the AAA client can be running either RADIUS or TACACS+; and the AAA client must be using Cisco IOS Release 11.2.7 or later and be configured to send a watchdog accounting packet (aaa accounting new-info update) with the IP address of



Downloaded from www.Manualslib.com manuals search engine

the calling station. (Watchdog packets are interim packets sent periodically during a session. They provide an approximate session length in the event that no stop packet is received to mark the end of the session.)

You can control whether Cisco Secure ACS propagates passwords changed by this feature. For more information, see Local Password Management, page 8-5.

Cisco Secure ACS supports password aging using the RADIUS protocol under MS CHAP versions 1 and 2. Cisco Secure ACS does not support password aging over Telnet connections using the RADIUS protocol.

**Caution** If a user with a RADIUS connection tries to make a Telnet connection to the AAA client during or after the password aging warning or grace period, the change password option does not appear, and the user account is expired.

### Password Aging Feature Settings

This section details only the Password Aging for Device-hosted Sessions and Password Aging for Transit Sessions mechanisms. For information on the Windows Password Aging mechanism, see Enabling Password Aging for Users in Windows Databases, page 6-26. For information on configuring local password validation options, see Local Password Management, page 8-5.

**Note** The password aging feature does not operate correctly if you also use the callback feature. When callback is used, users cannot receive password aging messages at login.

The password aging feature in Cisco Secure ACS has the following options:

- **Apply age-by-date rules**—Selecting this check box configures Cisco Secure ACS to determine password aging by date. The age-by-date rules contain the following settings:
  - **Active period**—The number of days users will be allowed to log in before being prompted to change their passwords. For example, if you enter 20, users can use their passwords for 20 days without being prompted to change them. The default Active period is 20 days.
  - **Warning period**—The number of days users will be notified to change their passwords. The existing password can be used, but the Cisco Secure ACS presents a warning indicating that the password must be changed



Downloaded from www.Manualslib.com manuals search engine

and displays the number of days left before the password expires. For example, if you enter 5 in this box and 20 in the Active period box, users will be notified to change their passwords on the 21st through 25th days.

- **Grace period**—The number of days to provide as the user grace period. The grace period allows a user to log in once to change the password. The existing password can be used one last time after the number of days specified in the active and warning period fields has been exceeded. Then, a dialog box warns the user that the account will be disabled if the password is not changed, and enables the user to change it. Continuing with the examples above, if you allow a 5-day grace period, a user who did not log in during the active and warning periods would be permitted to change passwords up to and including the 30th day. However, even though the grace period is set for 5 days, a user is allowed only one attempt to change the password when the password is in the grace period. Cisco Secure ACS displays the "last chance" warning only once. If the user does not change the password, this login is still permitted, but the password expires, and the next authentication is denied. An entry is logged in the Failed-Attempts log, and the user must contact an administrator to have the account reinstated.

**Note** All passwords expire at midnight, not the time at which they were set.

- **Apply age-by-uses rules**—Selecting this check box configures Cisco Secure ACS to determine password aging by the number of logins. The age-by-uses rules contain the following settings:
  - **Issue warning after** *x* **logins**—The number of the login upon which Cisco Secure ACS begins prompting users to change their passwords. For example, if you enter 10, users are allowed to log in 10 times without a change-password prompt. On the 11th login, they are prompted to change their passwords.

**Tip** To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

  - **Require change after** *x* **logins**—The number of the login after which to notify users that they must to change their passwords. Continuing with the previous example, if this number is set to 12, users receive prompts



Downloaded from www.Manualslib.com manuals search engine

requesting them to change their passwords on their 11th and 12th login attempts. On the 13th login attempt, they receive a prompt telling them that they must change their passwords. If users do not change their passwords now, their accounts expire and they cannot log in. This number must be greater than the **Issue warning after** *x* **login** number.

**Tip** To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

- **Apply password change rule**—Selecting this check box forces new users to change their passwords the first time they log in.
- **Generate greetings for successful logins**—Selecting this check box enables a Greetings message to display whenever users log in successfully via the CAA client. The message contains up-to-date password information specific to this user account.

The password aging rules are not mutually exclusive; a rule is applied for each check box that is selected. For example, users can be forced to change their passwords every 20 days, and every 10 logins, and to receive warnings and grace periods accordingly.

If no options are selected, passwords never expire.

Unlike most other parameters, which have corresponding settings at the user level, password aging parameters are configured only on a group basis.

Users who fail authentication because they have not changed their passwords and have exceeded their grace periods are logged in the Failed Attempts log. The accounts expire and appear in the Accounts Disabled list.

**Before You Begin**

- Verify that your AAA client is running the TACACS+ or RADIUS protocol. (TACACS+ only supports password aging for device-hosted sessions.)
- Set up your AAA client to perform authentication *and* accounting using the same protocol, either TACACS+ or RADIUS.
- Verify that you have configured your password validation options. For more information, see Local Password Management, page 8-5.
- Set up your AAA client to use Cisco IOS Release 11.2.7 or later and to send a watchdog accounting packet (aaa accounting new-info update) with the IP address of the calling station.



Downloaded from www.Manualslib.com manuals search engine

To set password aging rules for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** From the Jump To list at the top of the page, choose **Password Aging**.

The Password Aging Rules table appears.

**Step 4** To set password aging by date, select the **Apply age-by-date rules** check box and type the number of days for the following options, as applicable:

- Active period
- Warning period
- Grace period

**Note** Up to 5 characters are allowed in each field.

**Step 5** To set password aging by use, select the **Apply age-by-uses rules** check box and type the number of logins for each of the following options, as applicable:

- Issue warning after *x* logins
- Require change after *x* logins

**Note** Up to 5 characters are allowed in each field.

**Step 6** To force the user to change the password on the first login after an administrator has changed it, select the **Apply password change rule** check box.

**Step 7** To enable a Greetings message display, select the **Generate greetings for successful logins** check box.



Downloaded from www.Manualslib.com manuals search engine

**Step 8** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 9** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Enabling Password Aging for Users in Windows Databases

Cisco Secure ACS supports two types of password aging for users in Windows databases. Both types of Windows password aging mechanisms are separate and distinct from the other Cisco Secure ACS password aging mechanisms. For information on the requirements and settings for the password aging mechanisms that control users in the CiscoSecure user database, see Enabling Password Aging for the CiscoSecure User Database, page 6-21.

**Note** You can run both Windows Password Aging and Cisco Secure ACS Password Aging for Transit Sessions mechanisms concurrently, provided that the users authenticate from the two different databases.

The types of password aging in Windows databases are as follows:

- **RADIUS-based password aging**—RADIUS-based password aging depends upon the RADIUS AAA protocol to send and receive the password change messages. Requirements for implementing the RADIUS-based Windows password aging mechanism include the following:
  - Communication between Cisco Secure ACS and the AAA client must be using RADIUS.
  - The AAA client must support MS CHAP password aging in addition to MS CHAP authentication.
  - Users must be in a Windows user database.
  - Users must be using the Windows DUN client.
  - You must enable MS CHAP version 1 or MS CHAP version 2, or both, in the Windows configuration within the External User Databases section.



Downloaded from www.Manualslib.com manuals search engine

**Tip** For information on enabling MS CHAP for password changes, see Configuring a Windows External User Database, page 13-30. For information on enabling MS CHAP in System Configuration, see Global Authentication Setup, page 10-26.

- **PEAP password aging**—PEAP password aging depends upon the PEAP(EAP-GTC) or PEAP(EAP-MSCHAPv2) authentication protocol to send and receive the password change messages. Requirements for implementing the PEAP Windows password aging mechanism include the following:
  - The AAA client must support EAP.
  - Users must be in a Windows user database.
  - Users must be using a Microsoft PEAP client, such as Windows XP.
  - You must enable PEAP on the Global Authentication Configuration page within the System Configuration section.

**Tip** For information about enabling PEAP in System Configuration, see Global Authentication Setup, page 10-26.

  - You must enable PEAP password changes on the Windows Authentication Configuration page within the External User Databases section.

**Tip** For information about enabling PEAP password changes, see Windows User Database, page 13-7.

- **EAP-FAST password aging**—If password aging occurs during phase zero of EAP-FAST, it depends upon EAP-MSCHAPv2 to send and receive the password change messages. If password aging occurs during phase two of EAP-FAST, it depends upon EAP-GTC to send and receive the password change messages. Requirements for implementing the EAP-FAST Windows password aging mechanism include the following:
  - The AAA client must support EAP.
  - Users must be in a Windows user database.



Downloaded from www.Manualslib.com manuals search engine

- Users must be using a client that supports EAP-FAST.
- You must enable EAP-FAST on the Global Authentication Configuration page within the System Configuration section.

**Tip** For information about enabling EAP-FAST in System Configuration, see Global Authentication Setup, page 10-26.

- You must enable EAP-FAST password changes on the Windows Authentication Configuration page within the External User Databases section.

**Tip** For information about enabling EAP-FAST password changes, see Windows User Database, page 13-7.

Users whose Windows accounts reside in "remote" domains (that is, not the domain within which Cisco Secure ACS is running) can only use the Windows-based password aging if they supply their domain names.

The methods and functionality of Windows password aging differ according to which Microsoft Windows operating system you are using, and whether you employ Active Directory (AD) or Security Accounts Manager (SAM). Setting password aging for users in the Windows user database is only one part of the larger task of setting security policies in Windows. For comprehensive information on Windows procedures, refer to your Windows system documentation.

# Setting IP Address Assignment Method for a User Group

Perform this procedure to configure the way Cisco Secure ACS assigns IP addresses to users in the group. The four possible methods are as follows:

- **No IP address assignment**—No IP address is assigned to this group.
- **Assigned by dialup client**—Use the IP address that is configured on the dialup client network settings for TCP/IP.



Downloaded from www.Manualslib.com manuals search engine

- **Assigned from AAA Client pool**—The IP address is assigned by an IP address pool assigned on the AAA client.
- **Assigned from AAA server pool**—The IP address is assigned by an IP address pool assigned on the AAA server.

To set an IP address assignment method for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** From the Jump To list at the top of the page, choose **IP Address Assignment**.

**Step 4** In the IP Assignment table, do one of the following:

- Select **No IP address assignment**.
- Select **Assigned by dialup client**.
- Select **Assigned from AAA Client pool**. Then, type the AAA client IP pool name.
- Select **Assigned from AAA pool**. Then, select the AAA server IP pool name in the Available Pools list and click **-->** (right arrow button) to move the name into the Selected Pools list.

**Note** If there is more than one pool in the Selected Pools list, the users in this group are assigned to the first available pool in the order listed.

**Tip** To change the position of a pool in the list, select the pool name and click **Up** or **Down** until the pool is in the position you want.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Assigning a Downloadable IP ACL to a Group

The Downloadable ACLs feature enables you to assign an IP ACL at the group level.

**Note** You must have established one or more IP ACLs before attempting to assign one. For instructions on how to add a downloadable IP ACL using the Shared Profile Components section of the Cisco Secure ACS HTML interface, see Adding a Downloadable IP ACL, page 5-10.

**Tip** The Downloadable ACLs table does not appear if it has not been enabled. To enable the Downloadable ACLs table, click **Interface Configuration**, click **Advanced Options**, and then select the **Group-Level Downloadable ACLs** check box.

To assign a downloadable IP ACL to a group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** From the Jump To list at the top of the page, choose **Downloadable ACLs**.

**Step 4** Under the Downloadable ACLs section, click the **Assign IP ACL** check box.

**Step 5** Select an IP ACL from the list.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Configuring TACACS+ Settings for a User Group

Perform this procedure to configure and enable the service/protocol parameters to be applied for the authorization of each user who belongs to the group. For information on how to configure settings for the Shell Command Authorization Set, see Configuring a Shell Command Authorization Set for a User Group, page 6-33.

**Note** To display or hide additional services or protocols, click **Interface Configuration**, click **TACACS+ (Cisco IOS)**, and then select or clear items in the group column, as applicable.

To configure TACACS+ settings for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

**Step 4** To configure services and protocols in the TACACS+ Settings table to be authorized for the group, follow these steps:

**a.** Select one or more service/protocol check boxes (for example, PPP IP or ARAP).

**b.** Under each service/protocol that you selected in Step a, select attributes and then type in the corresponding values, as applicable, to further define authorization for that service/protocol.



Downloaded from www.Manualslib.com manuals search engine

To employ custom attributes for a particular service, you must select the **Custom attributes** check box under that service, and then specify the attribute/value in the box below the check box.

For more information about attributes, see Appendix B, "TACACS+ Attribute-Value Pairs", or your AAA client documentation.

**Tip** For ACLs and IP address pools, the name of the ACL or pool as defined on the AAA client should be entered. (An ACL is a list of Cisco IOS commands used to restrict access to or from other devices and users on the network.)

**Note** Leave the attribute value box blank if the default (as defined on the AAA client) should be used.

**Note** You can define and download an ACL. Click **Interface Configuration**, click **TACACS+ (Cisco IOS)**, and then select **Display a window for each service selected in which you can enter customized TACACS+ attributes**. A box opens under each service/protocol in which you can define an ACL.

**Step 5** To allow all services to be permitted unless specifically listed and disabled, you can select the **Default (Undefined) Services** check box under the Checking this option will PERMIT all UNKNOWN Services table.

**Caution** This is an advanced feature and should only be used by administrators who understand the security implications.

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Configuring a Shell Command Authorization Set for a User Group

Use this procedure to specify the shell command authorization set parameters for a group. There are four options:

- **None**—No authorization for shell commands.
- **Assign a Shell Command Authorization Set for any network device**—One shell command authorization set is assigned, and it applies to all network devices.
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Enables you to associate particular shell command authorization sets to be effective on particular NDGs.
- **Per Group Command Authorization**—Enables you to permit or deny specific Cisco IOS commands and arguments at the group level.

**Note** This feature requires that you have previously configured a shell command authorization set. For detailed steps, see Adding a Command Authorization Set, page 5-31.

To specify shell command authorization set parameters for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

**Step 4** Use the vertical scrollbar to scroll to the Shell Command Authorization Set feature area.

**Step 5** To prevent the application of any shell command authorization set, select (or accept the default of) the **None** option.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** To assign a particular shell command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a Shell Command Authorization Set for any network device** option.

b. Then, from the list directly below that option, select the shell command authorization set you want applied to this group.

**Step 7** To create associations that assign a particular shell command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and a corresponding **Command Set**.

**Tip** You can select a **Command Set** that will be effective for all **Device Groups**, that are not otherwise assigned, by assigning that set to the <*default*> Device Group.

c. Click **Add Association**.

The associated NDG and shell command authorization set appear in the table.

**Step 8** To define the specific Cisco IOS commands and arguments to be permitted or denied at the group level, follow these steps:

a. Select the **Per Group Command Authorization** option.

b. Under Unmatched Cisco IOS commands, select either **Permit** or **Deny**.

If you select Permit, users can issue all commands not specifically listed. If you select Deny, users can issue only those commands listed.

c. To list particular commands to be permitted or denied, select the **Command** check box and then type the name of the command, define its arguments using standard permit or deny syntax, and select whether unlisted arguments should be permitted or denied.

**Caution** This is a powerful, advanced feature and should be used by an administrator skilled with Cisco IOS commands. Correct syntax is the responsibility of the administrator. For information on how Cisco Secure ACS uses pattern matching in command arguments, see About Pattern Matching, page 5-30.



Downloaded from www.Manualslib.com manuals search engine

**Tip** To enter several commands, you must click **Submit** after specifying a command. A new command entry box appears below the box you just completed.

# Configuring a PIX Command Authorization Set for a User Group

Use this procedure to specify the PIX command authorization set parameters for a user group. There are three options:

- **None**—No authorization for PIX commands.
- **Assign a PIX Command Authorization Set for any network device**—One PIX command authorization set is assigned, and it applies all network devices.
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command authorization sets are to be effective on particular NDGs.

**Before You Begin**

- Ensure that a AAA client has been configured to use TACACS+ as the security control protocol.
- On the TACACS+ (Cisco) page of Interface Configuration section, ensure that the PIX Shell (pixShell) option is selected in the Group column.
- Make sure that you have already configured one or more PIX command authorization sets. For detailed steps, see Adding a Command Authorization Set, page 5-31.

To specify PIX command authorization set parameters for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

**Step 4** Scroll down to the PIX Command Authorization Set feature area within the TACACS+ Settings table.

**Step 5** To prevent the application of any PIX command authorization set, select (or accept the default of) the **None** option.

**Step 6** To assign a particular PIX command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a PIX Command Authorization Set for any network device** option.

b. From the list directly below that option, select the PIX command authorization set you want applied to this user group.

**Step 7** To create associations that assign a particular PIX command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

The associated NDG and PIX command authorization set appear in the table.

**Note** To remove or edit an existing PIX command authorization set association, you can select the association from the list, and then click **Remove Association**.



Downloaded from www.Manualslib.com manuals search engine

# Configuring Device-Management Command Authorization for a User Group

Use this procedure to specify the device-management command authorization set parameters for a group. Device-management command authorization sets support the authorization of tasks in Cisco device-management applications that are configured to use Cisco Secure ACS for authorization. There are three options:

- **None**—No authorization is performed for commands issued in the applicable Cisco device-management application.
- **Assign a** *device-management application* for any network device—For the applicable device-management application, one command authorization set is assigned, and it applies to management tasks on all network devices.
- **Assign a** *device-management application* on a per Network Device Group Basis—For the applicable device-management application, this option enables you to apply command authorization sets to specific NDGs, so that it affects all management tasks on the network devices belonging to the NDG.

**Note** This feature requires that you have configured a command authorization set for the applicable Cisco device-management application. For detailed steps, see Adding a Command Authorization Set, page 5-31.

To specify device-management application command authorization for a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

**Step 4** Use the vertical scrollbar to scroll to the *device-management application* feature area, where *device-management application* is the name of the applicable Cisco device-management application.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** To prevent the application of any command authorization set for the applicable device-management application, select the **None** option.

**Step 6** To assign a particular command authorization set that affects device-management application actions on any network device, follow these steps:

a. Select the **Assign a** *device-management application* for any network device option.

b. Then, from the list directly below that option, select the command authorization set you want applied to this group.

**Step 7** To create associations that assign a particular command authorization set that affects device-management application actions on a particular NDG, for each association, follow these steps:

a. Select the **Assign a** *device-management application* on a per Network Device Group Basis option.

b. Select a **Device Group** and a corresponding **device-management application**.

c. Click **Add Association**.

The associated NDG and command authorization set appear in the table.

# Configuring IETF RADIUS Settings for a User Group

These parameters appear only when both the following are true:

- A AAA client has been configured to use one of the RADIUS protocols in Network Configuration.
- Group-level RADIUS attributes have been enabled on the RADIUS (IETF) page in the Interface Configuration section of the HTML interface.

RADIUS attributes are sent as a profile for each user from Cisco Secure ACS to the requesting AAA client. To display or hide any of these attributes, see Protocol Configuration Options for RADIUS, page 3-11. For a list and explanation of RADIUS attributes, see Appendix C, "RADIUS Attributes". For more information about how your AAA client uses RADIUS, refer to your AAA client vendor documentation.



Downloaded from www.Manualslib.com manuals search engine

To configure IETF RADIUS attribute settings to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 3** From the Jump To list at the top of the page, choose **RADIUS (IETF)**.

**Step 4** For each IETF RADIUS attribute you need to authorize for the current group, select the check box next to the attribute and then define the authorization for the attribute in the field or fields next to it.

**Step 5** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 6** To configure the vendor-specific attributes (VSAs) for any RADIUS network device vendor supported by Cisco Secure ACS, see the appropriate section:

- Configuring Cisco IOS/PIX RADIUS Settings for a User Group, page 6-40
- Configuring Cisco Aironet RADIUS Settings for a User Group, page 6-41
- Configuring Ascend RADIUS Settings for a User Group, page 6-43
- Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group, page 6-44
- Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 6-46
- Configuring Microsoft RADIUS Settings for a User Group, page 6-47
- Configuring Nortel RADIUS Settings for a User Group, page 6-49
- Configuring Juniper RADIUS Settings for a User Group, page 6-50
- Configuring BBSM RADIUS Settings for a User Group, page 6-51

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Configuring Cisco IOS/PIX RADIUS Settings for a User Group

The Cisco IOS/PIX RADIUS parameters appear only when both the following are true:

- A AAA client has been configured to use RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Cisco IOS/PIX) attributes have been enabled in Interface Configuration: RADIUS (Cisco IOS/PIX).

Cisco IOS/PIX RADIUS represents only the Cisco VSAs. You must configure both the IETF RADIUS and Cisco IOS/PIX RADIUS attributes.

**Note** To hide or display Cisco IOS/PIX RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco IOS/PIX RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** Before you configure Cisco IOS/PIX RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-38.

**Step 2** If you want to use the [009\001] cisco-av-pair attribute to specify authorizations, select the check box next to the attribute and then type the attribute-value pairs in the text box. Separate each attribute-value pair by pressing Enter.

For example, if the current group is used for assigning authorizations to Network Admission Control (NAC) clients to which Cisco Secure ACS assigns a system posture token of Infected, you could specify values for the url-redirect, posture-token, and status-query-timeout attributes as follows:

```
url-redirect=http://10.1.1.1
posture-token=Infected
status-query-timeout=150
```



Downloaded from www.Manualslib.com manuals search engine

**Step 3** If you want to use other Cisco IOS/PIX RADIUS attributes, select the corresponding check box and specify the required values in the adjacent text box.

**Step 4** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 5** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Configuring Cisco Aironet RADIUS Settings for a User Group

The single Cisco Aironet RADIUS VSA, Cisco-Aironet-Session-Timeout, is a virtual VSA. It is a specialized implementation of the IETF RADIUS Session-Timeout attribute (27) that Cisco Secure ACS uses only when it responds to a RADIUS request from a AAA client using RADIUS (Cisco Aironet). This enables you to provide different timeout values for users accessing your network through wireless and wired access devices. By specifying a timeout value specifically for WLAN connections, you avoid the difficulties that would arise if you had to use a standard timeout value (typically measured in hours) for a WLAN connection (that is typically measured in minutes).

**Tip** Only enable and configure the Cisco-Aironet-Session-Timeout when some or all members of a group may connect through wired or wireless access devices. If members of a group always connect with a Cisco Aironet Access Point (AP) or always connect only with a wired access device, you do not need to use Cisco-Aironet-Session-Timeout but should instead configure RADIUS (IETF) attribute 27, Session-Timeout.

Imagine a user group Cisco-Aironet-Session-Timeout set to 600 seconds (10 minutes) and that same user group IETF RADIUS Session-Timeout set to 3 hours. When a member of this group connects through a VPN concentrator, Cisco Secure ACS uses 3 hours as the timeout value. However, if that same user connects via a Cisco Aironet AP, Cisco Secure ACS responds to an authentication request from the Aironet AP by sending 600 seconds in the IETF RADIUS Session-Timeout attribute. Thus, with the Cisco-Aironet-Session-Timeout attribute configured, different session timeout values can be sent depending on whether the end-user client is a wired access device or a Cisco Aironet AP.



Downloaded from www.Manualslib.com manuals search engine

The Cisco-Aironet-Session-Timeout VSA appears on the Group Setup page only when both the following are true:

- A AAA client has been configured to use RADIUS (Cisco Aironet) in Network Configuration.
- The group-level RADIUS (Cisco Aironet) attribute has been enabled in Interface Configuration: RADIUS (Cisco Aironet).

**Note** To hide or display the Cisco Aironet RADIUS VSA, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients configured to use RADIUS (Cisco Aironet), the VSA settings do not appear in the group configuration interface.

To configure and enable the Cisco Aironet RADIUS attribute to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** Confirm that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-38.

**Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 3** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco Aironet)**.

**Step 5** In the Cisco Aironet RADIUS Attributes table, select the **[5842\001] Cisco-Aironet-Session-Timeout** check box.

**Step 6** In the [5842\001] Cisco-Aironet-Session-Timeout box, type the session timeout value (in seconds) that Cisco Secure ACS is to send in the IETF RADIUS Session-Timeout (27) attribute when the AAA client is configured in Network Configuration to use the RADIUS (Cisco Aironet) authentication option. The recommended value is 600 seconds.

For more information about the IETF RADIUS Session-Timeout attribute, see Appendix C, "RADIUS Attributes", or your AAA client documentation.



Downloaded from www.Manualslib.com manuals search engine

**Step 7** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 8** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Configuring Ascend RADIUS Settings for a User Group

The Ascend RADIUS parameters appear only when both the following are true:

- A AAA client has been configured to use RADIUS (Ascend) or RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Ascend) attributes have been enabled in Interface Configuration: RADIUS (Ascend).

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure both the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting displayed for RADIUS is `Ascend-Remote-Addr`.

**Note** To hide or display Ascend RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Ascend RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** Confirm that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-38.

**Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 4** From the Jump To list at the top of the page, choose **RADIUS (Ascend)**.

**Step 5** In the Ascend RADIUS Attributes table, determine the attributes to be authorized for the group by selecting the check box next to the attribute. Be sure to define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or your AAA client documentation.

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Configuring Cisco VPN 3000 Concentrator RADIUS Settings for a User Group

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, Cisco Secure ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the Cisco Secure ACS HTML interface or how those attributes might be configured.

The Cisco VPN 3000 Concentrator RADIUS attribute configurations appear only if both the following are true:

- A AAA client has been configured to use RADIUS (Cisco VPN 3000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 3000) attributes have been enabled on the RADIUS (Cisco VPN 3000) page of the Interface Configuration section.



Downloaded from www.Manualslib.com manuals search engine

Cisco VPN 3000 Concentrator RADIUS represents only the Cisco VPN 3000 Concentrator VSA. You must configure both the IETF RADIUS and Cisco VPN 3000 Concentrator RADIUS attributes.

**Note** To hide or display Cisco VPN 3000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco VPN 3000 Concentrator RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-38.

**Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 3** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 3000)**.

**Step 5** In the Cisco VPN 3000 Concentrator RADIUS Attributes table, determine the attributes to be authorized for the group by selecting the check box next to the attribute. Further define the authorization for that attribute in the field next to it.

For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group

The Cisco VPN 5000 Concentrator RADIUS attribute configurations display only when both the following are true:

- A network device has been configured to use RADIUS (Cisco VPN 5000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 5000) attributes have been enabled on the RADIUS (Cisco VPN 5000) page of the Interface Configuration section.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSA. You must configure both the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.

**Note** To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-38.

**Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 3** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 5000)**.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** In the Cisco VPN 5000 Concentrator RADIUS Attributes table, select the attributes that should be authorized for the group by selecting the check box next to the attribute. Further define the authorization for each attribute in the field next to it.

For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Configuring Microsoft RADIUS Settings for a User Group

Microsoft RADIUS provides VSAs supporting MPPE, which is an encryption technology developed by Microsoft to encrypt PPP links. These PPP connections can be via a dial-in line, or over a VPN tunnel.

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, Cisco Secure ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the Cisco Secure ACS HTML interface or how those attributes might be configured.

The Microsoft RADIUS attribute configurations appear only when both the following are true:

- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the Microsoft RADIUS VSA.
- Group-level Microsoft RADIUS attributes have been enabled on the RADIUS (Microsoft) page of the Interface Configuration section.



Downloaded from www.Manualslib.com manuals search engine

The following Cisco Secure ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS/PIX
- Cisco VPN 3000
- Ascend

Microsoft RADIUS represents only the Microsoft VSA. You must configure both the IETF RADIUS and Microsoft RADIUS attributes.

**Note** To hide or display Microsoft RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Microsoft RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-38.

**Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 3** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 4** From the Jump To list at the top of the page, choose **RADIUS (Microsoft)**.

**Step 5** In the Microsoft RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.



Downloaded from www.Manualslib.com manuals search engine

**Note** The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Configuring Nortel RADIUS Settings for a User Group

The Nortel RADIUS attribute configurations appear only when both the following are true:

- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the Nortel RADIUS VSA.
- Group-level Nortel RADIUS attributes have been enabled on the RADIUS (Nortel) page of the Interface Configuration section.

Nortel RADIUS represents only the Nortel VSA. You must configure both the IETF RADIUS and Nortel RADIUS attributes.

**Note** To hide or display Nortel RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Nortel RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-38.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 3** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 4** From the Jump To list at the top of the page, choose **RADIUS (Nortel)**.

**Step 5** In the Nortel RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

**Note** The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Configuring Juniper RADIUS Settings for a User Group

Juniper RADIUS represents only the Juniper VSA. You must configure both the IETF RADIUS and Juniper RADIUS attributes.

**Note** To hide or display Juniper RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.



Downloaded from www.Manualslib.com manuals search engine

To configure and enable Juniper RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-38.

**Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 3** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 4** From the Jump To list at the top of the page, choose **RADIUS (Juniper)**.

**Step 5** In the Juniper RADIUS Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

**Note** The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Configuring BBSM RADIUS Settings for a User Group

BBSM RADIUS represents only the BBSM RADIUS VSA. You must configure both the IETF RADIUS and BBSM RADIUS attributes.



Downloaded from www.Manualslib.com manuals search engine

**Note** To hide or display BBSM RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable BBSM RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-38.

**Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 3** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 4** From the Jump To list at the top of the page, choose **RADIUS (BBSM)**.

**Step 5** In the BBSM RADIUS Attributes table, specify the attribute to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

**Note** The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Configuring Custom RADIUS VSA Settings for a User Group

User-defined, custom Radius VSA configurations appear only when all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-28.)
- A network device has been configured in Network Configuration that uses a RADIUS protocol that supports the custom VSA.
- Group-level custom RADIUS attributes have been enabled on the RADIUS (*Name*) page of the Interface Configuration section.

You must configure both the IETF RADIUS and the custom RADIUS attributes.

To configure and enable custom RADIUS attributes to be applied as an authorization for each user in the current group, follow these steps:

**Step 1** Confirm that your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Configuring IETF RADIUS Settings for a User Group, page 6-38.

**Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 3** From the Group list, select a group, and then click **Edit Settings**.

The Group Settings page displays the name of the group at its top.

**Step 4** From the Jump To list at the top of the page, choose **RADIUS (***custom name***)**.

**Step 5** In the RADIUS (*custom name*) Attributes table, specify the attributes to be authorized for the group by selecting the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see Appendix C, "RADIUS Attributes", or the documentation for network devices using RADIUS.

**Note** The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** To save the group settings you have just made, click **Submit**.

For more information, see Saving Changes to User Group Settings, page 6-56.

**Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

# Group Setting Management

This section describes how to use the Group Setup section to perform a variety of managerial tasks.

This section contains the following topics:


- Listing Users in a User Group, page 6-54
- Resetting Usage Quota Counters for a User Group, page 6-55
- Renaming a User Group, page 6-55
- Saving Changes to User Group Settings, page 6-56


## Listing Users in a User Group

To list all users in a specified group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select the group.

**Step 3** Click **Users in Group**.

The User List page for the particular group selected opens in the display area.

**Step 4** To open a user account (to view, modify, or delete a user), click the name of the user in the User List.

The User Setup page for the particular user account selected appears.



Downloaded from www.Manualslib.com manuals search engine

# Resetting Usage Quota Counters for a User Group

You can reset the usage quota counters for all members of a group, either before or after a quota has been exceeded.

To reset usage quota counters for all members of a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select the group.

**Step 3** In the Usage Quotas section, select the **On submit reset all usage counters for all users of this group** check box.

**Step 4** Click **Submit** at the bottom of the browser page.

The usage quota counters for all users in the group are reset. The Group Setup Select page appears.

# Renaming a User Group

To rename a user group, follow these steps:

**Step 1** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

**Step 2** From the Group list, select the group.

**Step 3** Click **Rename Group**.

The Renaming Group: *Group Name* page appears.

**Step 4** Type the new name in the **Group** field. Group names cannot contain angle brackets (< or >).



Downloaded from www.Manualslib.com manuals search engine

**Step 5** Click **Submit**.

**Note** The group remains in the same position in the list. The number value of the group is still associated with this group name. Some utilities, such as the database import utility, use the numeric value associated with the group.

The Select page opens with the new group name selected.

# Saving Changes to User Group Settings

After you have completed configuration for a group, be sure to save your work.

To save the configuration for the current group, follow these steps:

**Step 1** To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, and then click **Service Control**, and click **Restart**.

**Tip** To save your changes and apply them immediately, click **Submit + Restart**.

The group attributes are applied and services are restarted. The Edit page opens.

**Note** Restarting the service clears the Logged-in User Report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter.

**Step 2** To verify that your changes were applied, select the group and click **Edit Settings**. View the settings.



Downloaded from www.Manualslib.com manuals search engine

# User Management

This chapter provides information about setting up and managing user accounts in Cisco Secure ACS for Windows Server.

**Note** Settings at the user level override settings configured at the group level.

Before you configure User Setup, you should understand how this section functions. Cisco Secure ACS dynamically builds the User Setup section interface depending on the configuration of your AAA client and the security protocols being used. That is, what you see under User Setup is affected by settings in both the Network Configuration and Interface Configuration sections.

This chapter contains the following topics:


- About User Setup Features and Functions, page 7-1
- About User Databases, page 7-2
- Basic User Setup Options, page 7-3
- Advanced User Authentication Settings, page 7-22
- User Management, page 7-54


## About User Setup Features and Functions

The User Setup section of the Cisco Secure ACS HTML interface is the centralized location for all operations regarding user account configuration and administration.



Downloaded from www.Manualslib.com manuals search engine

From within the User Setup section, you can perform the following tasks:

- View a list of all users in the CiscoSecure user database.
- Find a user.
- Add a user.
- Assign the user to a group, including Voice-over-IP (VoIP) Groups.
- Edit user account information.
- Establish or change user authentication type.
- Configure callback information for the user.
- Set network access restrictions (NARs) for the user.
- Configure Advanced Settings.
- Set the maximum number of concurrent sessions (Max Sessions) for the user.
- Disable or re-enable the user account.
- Delete the user.

# About User Databases

Cisco Secure ACS authenticates users against one of several possible databases, including its CiscoSecure user database. Regardless of which database you configure Cisco Secure ACS to use when authenticating a user, all users have accounts within the CiscoSecure user database, and authorization of users is always performed against the user records in the CiscoSecure user database. The following list details the basic user databases used and provides links to greater details on each:

- **CiscoSecure user database**—Authenticates a user from the local CiscoSecure user database. For more information, see CiscoSecure User Database, page 13-2.

**Tip** The following authentication types appear in the HTML interface only when the corresponding external user database has been configured in the Database Configuration area of the External User Databases section.



Downloaded from www.Manualslib.com manuals search engine

- **Windows Database**—Authenticates a user with an existing account in the Windows user database located in the local domain or in domains configured in the Windows user database. For more information, see Windows User Database, page 13-7.
- **Generic LDAP**—Authenticates a user from a Generic LDAP external user database. For more information, see Generic LDAP, page 13-32.
- **Novell NDS**—Authenticates a user using Novell NetWare Directory Services (NDS). For more information, see Novell NDS Database, page 13-49.
- **ODBC Database**—Authenticates a user from an Open Database Connectivity-compliant database server. For more information, see ODBC Database, page 13-55.
- **LEAP Proxy RADIUS Server Database**—Authenticates a user from an LEAP Proxy RADIUS server. For more information, see LEAP Proxy RADIUS Server Database, page 13-75.
- **Token Server**—Authenticates a user from a token server database. Cisco Secure ACS supports the use of a variety of token servers for the increased security provided by one-time passwords. For more information, see Token Server User Databases, page 13-78

# Basic User Setup Options

This section presents the basic activities you perform when configuring a new user. At its most basic level, configuring a new user requires only three steps, as follows:

- Specify a name.
- Specify either an external user database or a password.
- Submit the information.

The steps for editing user account settings are essentially identical to those used when adding a user account but, to edit, you navigate directly to the field or fields to be changed. You cannot edit the name associated with a user account; to change a username you must delete the user account and establish another.

What other procedures you perform when setting up new user accounts is a function both of the complexity of your network and of the granularity of control you desire.



Downloaded from www.Manualslib.com manuals search engine

This section contains the following topics:


- Adding a Basic User Account, page 7-4
- Setting Supplementary User Information, page 7-6
- Setting a Separate CHAP/MS-CHAP/ARAP Password, page 7-7
- Assigning a User to a Group, page 7-8
- Setting User Callback Option, page 7-9
- Assigning a User to a Client IP Address, page 7-10
- Setting Network Access Restrictions for a User, page 7-11
- Setting Max Sessions Options for a User, page 7-16
- Setting User Usage Quotas Options, page 7-18
- Setting Options for User Account Disablement, page 7-20
- Assigning a Downloadable IP ACL to a User, page 7-21


# Adding a Basic User Account

This procedure details the minimum steps necessary to add a new user account to the CiscoSecure user database.

To add a user account, follow these steps:

**Step 1** In the navigation bar, click **User Setup**.

The User Setup Select page opens.

**Step 2** Type a name in the User box.

**Note** The username can contain up to 64 characters. Names cannot contain the following special characters:
# ? " * > <
Leading and trailing spaces are not allowed.

**Step 3** Click **Add/Edit**.

The User Setup Edit page opens. The username being added is at the top of the page.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** Make sure that the Account Disabled check box is cleared.

**Note** Alternatively, you can select the **Account Disabled** check box to create a user account that is disabled, and enable the account at another time.

**Step 5** Under Password Authentication in the User Setup table, select the applicable authentication type from the list.

**Tip** The authentication types that appear reflect the databases that you have configured in the Database Configuration area of the External User Databases section.

**Step 6** Specify a single CiscoSecure PAP password by typing it in the first set of **Password** and **Confirm Password** boxes.

**Note** Up to 32 characters are allowed each for the Password box and the Confirm Password box.

**Tip** The CiscoSecure PAP password is also used for CHAP/MS-CHAP/ARAP if the Separate CHAP/MS-CHAP/ARAP check box is not selected.

**Tip** You can configure the AAA client to ask for a PAP password first and then a CHAP or MS-CHAP password so that when users dial in using a PAP password, they will authenticate. For example, the following line in the AAA client configuration file causes the AAA client to enable CHAP after PAP:
**ppp authentication pap chap**

**Step 7** Do one of the following:

- To finish configuring the user account options and establish the user account, click **Submit**.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

**Tip** For lengthy account configurations, you can click **Submit** before continuing. This will prevent loss of information you have already entered if an unforeseen problem occurs.

# Setting Supplementary User Information

Supplementary User Information can contain up to five fields that you configure. The default configuration includes two fields: Real Name and Description.

For information about how to display and configure these optional fields, see User Data Configuration Options, page 3-3.

To enter optional information into the Supplementary User Information table, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Complete each box that appears in the Supplementary User Info table.

**Note** Up to 128 characters are allowed each for the Real Name and the Description boxes.

**Step 3** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Setting a Separate CHAP/MS-CHAP/ARAP Password

Setting a separate CHAP/MS-CHAP/ARAP password adds more security to Cisco Secure ACS authentication. However, you must have a AAA client configured to support the separate password.

To allow the user to authenticate using a CHAP, MS-CHAP, or ARAP password, instead of the PAP password in the CiscoSecure user database, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Select the **Separate CHAP/MS-CHAP/ARAP** check box in the User Setup table.

**Step 3** Specify the CHAP/MS-CHAP/ARAP password to be used by typing it in each of the second set of Password/Confirm boxes under the Separate (CHAP/MS-CHAP/ARAP) check box.

**Note** Up to 32 characters are allowed each for the Password box and the Confirm Password box.

**Note** These Password and Confirm Password boxes are only required for authentication by the Cisco Secure ACS database. Additionally, if a user is assigned to a VoIP (null password) group, and the optional password is also included in the user profile, the password is not used until the user is re-mapped to a non-VoIP group.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Assigning a User to a Group

A user can only belong to one group in Cisco Secure ACS. The user inherits the attributes and operations assigned to his or her group. However, in the case of conflicting settings, the settings at the user level override the settings configured at the group level.

By default, users are assigned to the Default Group. Users who authenticate via the Unknown User method and who are not mapped to an existing Cisco Secure ACS group are also assigned to the Default Group.

Alternatively, you can choose not to map a user to a particular group, but rather, to have the group mapped by an external authenticator. For external user databases from which Cisco Secure ACS can derive group information, you can associate the group memberships—defined for the users in the external user database—to specific Cisco Secure ACS groups. For more information, see Chapter 16, "User Group Mapping and Specification".

To assign a user to a group, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited appears at the top of the page.

**Step 2** From the Group to which user is assigned list in the User Setup table, select the group to which you want to assign the user.

**Tip** Alternatively, you can scroll up in the list to select the **Mapped By External Authenticator** option.

**Step 3** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Setting User Callback Option

Callback is a command string that is passed to the access server. You can use a callback string to initiate a modem to call the user back on a specific number for added security or reversal of line charges.

To set the user callback option, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited appears at the top of the page.

**Step 2** Under Callback in the User Setup table, select the applicable option. Choices include the following:

- **Use group setting**—Select if you want this user to use the setting for the group.
- **No callback allowed**—Select to disable callback for this user.
- **Callback using this number**—Select and type the complete number, including area code if necessary, on which to always call back this user.

**Note** The maximum character length for the callback number is 199 characters.

- **Dialup client specifies callback number**—Select to enable the Windows dialup client to specify the callback number.
- **Use Windows Database callback settings**—Select to use the settings specified for Windows callback. If a Windows account for a user resides in a remote domain, the domain in which Cisco Secure ACS resides must have a two-way trust with that domain for the Microsoft Windows callback settings to operate for that user.

**Note** The dial-in user must have configured software that supports callback.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

# Assigning a User to a Client IP Address

To assign a user to a client IP address, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Under Client IP Address Assignment in the User Setup table, select the applicable option. Choices include the following:

**Note** The IP address assignment in User Setup overrides the IP address assignment in Group Setup.

- **Use group settings**—Select this option to use the IP address group assignment.
- **No IP address assignment**—Select this option to override the group setting if you do not want an IP address returned by the client.
- **Assigned by dialup client**—Select this option to use the IP address dialup client assignment.
- **Assign static IP address**—Select this option and type the IP address in the box (up to 15 characters), if a specific IP address should be used for this user.

**Note** If the IP address is being assigned from a pool of IP addresses or by the dialup client, leave the Assign IP address box blank.



Downloaded from www.Manualslib.com manuals search engine

- **Assigned by AAA client pool**—Select this option and type the AAA client IP pool name in the box, if this user is to have the IP address assigned by an IP address pool configured on the AAA client.
- **Assigned from AAA pool**—Select this option and type the applicable pool name in the box, if this user is to have the IP address assigned by an IP address pool configured on the AAA server. Select the AAA server IP pool name from the Available Pools list, and then click **-->** (right arrow button) to move the name into the Selected Pools list. If there is more than one pool in the Selected Pools list, the users in this group are assigned to the first available pool in the order listed. To move the position of a pool in the list, select the pool name and click **Up** or **Down** until the pool is in the position you want.

**Step 3** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

# Setting Network Access Restrictions for a User

The Network Access Restrictions table in the Advanced Settings area of User Setup enables you to set NARs in three distinct ways:

- Apply existing shared NARs by name.
- Define IP-based access restrictions to permit or deny user access to a specified AAA client or to specified ports on a AAA client when an IP connection has been established.
- Define CLI/DNIS-based access restrictions to permit or deny user access based on the CLI/DNIS used.

**Note** You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see About Network Access Restrictions, page 5-15.



Downloaded from www.Manualslib.com manuals search engine

Typically, you define (shared) NARs from within the Shared Components section so that these restrictions can be applied to more than one group or user. For more information, see Adding a Shared Network Access Restriction, page 5-19. You must have selected the User-Level Shared Network Access Restriction check box on the Advanced Options page of the Interface Configuration section for this set of options to appear in the HTML interface.

However, Cisco Secure ACS also enables you to define and apply a NAR for a single user from within the User Setup section. You must have enabled the User-Level Network Access Restriction setting on the Advanced Options page of the Interface Configuration section for single user IP-based filter options and single user CLI/DNIS-based filter options to appear in the HTML interface.

**Note** When an authentication request is forwarded by proxy to a Cisco Secure ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

When you create access restrictions on a per-user basis, Cisco Secure ACS does not enforce limits to the number of access restrictions and it does not enforce a limit to the length of each access restriction; however, there are strict limits, as follows.

- The combination of fields for each line item cannot exceed 1024 characters in length.
- The shared NAR cannot have more than 16 KB of characters. The number of line items supported depends on the length of each line item. For example, if you create a CLI/DNIS-based NAR where the AAA client names are 10 characters, the port numbers are 5 characters, the CLI entries are 15 characters, and the DNIS entries are 20 characters, you can add 450 line items before reaching the 16 KB limit.

To set NARs for a user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** To apply a previously configured shared NAR to this user, follow these steps:

**Note** To apply a shared NAR, you must have configured it under Network Access Restrictions in the Shared Profile Components section. For more information, see Adding a Shared Network Access Restriction, page 5-19.

a. Select the **Only Allow network access when** check box.

b. To specify whether one or all shared NARs must apply for the user to be permitted access, select one of the following two options, as applicable:

- All selected NARS result in permit
- Any one selected NAR results in permit

c. Select a shared NAR name in the NARs list, and then click **-->** (right arrow button) to move the name into the Selected NARs list.

**Tip** To view the server details of the shared NARs you have selected to apply, you can click either **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

**Step 3** To define and apply a NAR, for this particular user, that permits or denies this user access based on IP address, or IP address and port, follow these steps:

**Tip** You should define most NARs from within the Shared Components section so that they can be applied to more than one group or user. For more information, see Adding a Shared Network Access Restriction, page 5-19.

a. In the Network Access Restrictions table, under Per User Defined Network Access Restrictions, select the **Define IP-based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select one of the following:

- Permitted Calling/Point of Access Locations
- Denied Calling/Point of Access Locations



Downloaded from www.Manualslib.com manuals search engine

c. Select or enter the information in the following boxes:

- **AAA Client**—Select **All AAA Clients**, or the name of a network device group (NDG), or the name of the individual AAA client, to which to permit or deny access.
- **Port**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports on the selected AAA client.
- **Address**—Type the IP address or addresses to use when performing access restrictions. You can use the wildcard asterisk (*).

**Note** The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.

d. Click **enter**.

The specified AAA client, port, and address information appears in the table above the AAA Client list.

**Step 4** To permit or deny this user access based on calling location or values other than an established IP address, follow these steps:

a. Select the **Define CLI/DNIS based access restrictions** check box.

b. To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one of the following:

- Permitted Calling/Point of Access Locations
- Denied Calling/Point of Access Locations



Downloaded from www.Manualslib.com manuals search engine

c. Complete the following boxes:

**Note** You must make an entry in each box. You can use the wildcard asterisk (*) for all or part of a value. The format you use must match the format of the string you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **AAA Client**—Select **All AAA Clients**, or the name of the NDG, or the name of the individual AAA client, to which to permit or deny access.
- **PORT**—Type the number of the port to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the wildcard asterisk (*) to permit or deny access based on part of the number.

**Tip** This is also the selection to use if you want to restrict access based on other values such as a Cisco Aironet client MAC address. For more information, see About Network Access Restrictions, page 5-15.

- **DNIS**—Type the DNIS number to which to permit or deny access. Use this to restrict access based on the number into which the user will be dialing. You can use the wildcard asterisk (*) to permit or deny access based on part of the number.

**Tip** This is also the selection to use if you want to restrict access based on other values such as a Cisco Aironet AP MAC address. For more information, see About Network Access Restrictions, page 5-15.

**Note** The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although Cisco Secure ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and Cisco Secure ACS cannot accurately apply it to users.



Downloaded from www.Manualslib.com manuals search engine

d. Click **enter**.

The information, specifying the AAA client, port, CLI, and DNIS, appears in the table above the AAA Client list.

**Step 5** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

# Setting Max Sessions Options for a User

The Max Sessions feature enables you to set the maximum number of simultaneous connections permitted for this user. For Cisco Secure ACS purposes, a session is considered any type of user connection supported by RADIUS or TACACS+, for example PPP, or Telnet, or ARAP. Note, however, that accounting must be enabled on the AAA client for Cisco Secure ACS to be aware of a session. All session counts are based on user and group names only. Cisco Secure ACS does not support any differentiation by type of session—all sessions are counted as the same. To illustrate, a user with a Max Session count of 1 who is dialed in to a AAA client with a PPP session will be refused a connection if that user then tries to Telnet to a location whose access is controlled by the same Cisco Secure ACS.

**Note** Each Cisco Secure ACS holds its own Max Sessions counts. There is no mechanism for Cisco Secure ACS to share Max Sessions counts across multiple Cisco Secure ACSes. Therefore, if two Cisco Secure ACS are set up as a mirror pair with the workload distributed between them, they will have completely independent views of the Max Sessions totals.

**Tip** If the Max Sessions table does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Max Sessions** check box.



Downloaded from www.Manualslib.com manuals search engine

To set max sessions options for a user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** In the Max Sessions table, under Sessions available to user, select one of the following three options:

- **Unlimited**—Select to allow this user an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
- *n*—Select and then type the maximum number of simultaneous sessions to allow this user.
- **Use group setting**—Select to use the Max Sessions value for the group.

**Note** The default setting is Use group setting.

**Note** User Max Sessions settings override the group Max Sessions settings. For example, if the group Sales has a Max Sessions value of only 10, but a user in the group Sales, John, has a User Max Sessions value of Unlimited, John is still allowed an unlimited number of sessions.

**Step 3** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Setting User Usage Quotas Options

You can define usage quotas for individual users. You can limit users in one or both of two ways:

- By total duration of sessions for the period selected.
- By the total number of sessions for the period selected.

For Cisco Secure ACS purposes, a session is considered any type of user connection supported by RADIUS or TACACS+, for example PPP, or Telnet, or ARAP. Note, however, that accounting must be enabled on the AAA client for Cisco Secure ACS to be aware of a session. If you make no selections in the Session Quotas section for an individual user, Cisco Secure ACS applies the session quotas of the group to which the user is assigned.

**Note** If the User Usage Quotas feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Usage Quotas** check box.

**Tip** The Current Usage table under the User Usage Quotas table on the User Setup Edit page displays usage statistics for the current user. The Current Usage table lists both online time and sessions used by the user, with columns for daily, weekly, monthly, and total usage. The Current Usage table appears only on user accounts that you have established; that is, it does not appear during initial user setup.

For a user who has exceeded his quota, Cisco Secure ACS denies him access upon his next attempt to start a session. If a quota is exceeded during a session, Cisco Secure ACS allows the session to continue. If a user account has been disabled because the user has exceeded usage quotas, the User Setup Edit page displays a message stating that the account has been disabled for this reason.

You can reset the session quota counters on the User Setup page for a user. For more information about resetting usage quota counters, see Resetting User Session Quota Counters, page 7-58.

To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated only when the user logs off. If the AAA client through which the user is accessing your network fails, the quota is not updated. In the case of multiple sessions, such as



Downloaded from www.Manualslib.com manuals search engine

with ISDN, the quota is not updated until all sessions terminate, which means that a second channel will be accepted even if the first channel has exhausted the quota allocated to the user.

To set usage quota options for a user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** In the Usage Quotas table, select **Use these settings**.

**Step 3** To define a usage quota based on duration of sessions for a user, follow these steps:

**a.** Select the **Limit user to** *x* **hours of online time** check box.

**b.** Type the number of hours to which you want to limit the user in the **Limit user to** *x* **hours of online time** box. Use decimal values to indicate minutes. For example, a value of 10.5 would equal 10 hours and 30 minutes.

**Note** Up to 10 characters are allowed for this field.

**c.** Select the period for which you want to enforce the time usage quota:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Absolute**—A continuous, open-ended count of hours.

**Step 4** To define usage quotas based on the number of sessions for a user, follow these steps:

**a.** Select the **Limit user to** *x* **sessions** check box.

**b.** Type the number of sessions to which you want to limit the user in the **Limit user to** *x* **sessions** box.

**Note** Up to 10 characters are allowed for this field.



Downloaded from www.Manualslib.com manuals search engine

c. Select the period for which you want to enforce the session usage quota:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Absolute**—A continuous, open-ended count of hours.

# Setting Options for User Account Disablement

The Account Disable feature defines the circumstances upon which a user account is disabled.

**Note** Do not confuse this feature with account expiration due to password aging. Password aging is defined for groups only, not for individual users. Also note that this feature is distinct from the Account Disabled check box. For instructions on how to disable a user account, see Disabling a User Account, page 7-56.

**Note** If the user is authenticated with a Windows user database, this expiration information is in addition to the information in the Windows user account. Changes here do not alter settings configured in Windows.

To set options for user account disablement, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Do one of the following:

a. Select the **Never** option to keep the user account always enabled.

**Note** This is the default setting.



Downloaded from www.Manualslib.com manuals search engine

b. Select the **Disable account if** option to disable the account under specific circumstances. Then, specify one or both of the circumstances under the following boxes:

- **Date exceeds**—Select the **Date exceeds:** check box. Then select the month and type the date (two characters) and year (four characters) on which to disable the account.

**Note** The default is 30 days after the user is added.

- **Failed attempts exceed**—Select the **Failed attempts exceed** check box and then type the number of consecutive unsuccessful login attempts to allow before disabling the account.

**Note** The default is 5.

**Step 3** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

# Assigning a Downloadable IP ACL to a User

The Downloadable ACLs feature enables you to assign an IP Access Control List (ACL) at the user level. You must configure one or more IP ACLs before you assign one. For instructions on how to configure a downloadable IP ACL using the Shared Profile Components section of the Cisco Secure ACS HTML interface, see Adding a Downloadable IP ACL, page 5-10.

**Note** The Downloadable ACLs table does not appear if it has not been enabled. To enable the Downloadable ACLs table, click **Interface Configuration**, click **Advanced Options**, and then select the **User-Level Downloadable ACLs** check box.



Downloaded from www.Manualslib.com manuals search engine

To assign a downloadable IP ACL to a user account, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added and edited is at the top of the page.

**Step 2** Under the Downloadable ACLs section, click the **Assign IP ACL:** check box.

**Step 3** Select an IP ACL from the list.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

# Advanced User Authentication Settings

This section presents the activities you perform to configure user-level TACACS+ and RADIUS enable parameters.

This section contains the following topics:


- TACACS+ Settings (User), page 7-23
  - Configuring TACACS+ Settings for a User, page 7-24
  - Configuring a Shell Command Authorization Set for a User, page 7-26
  - Configuring a PIX Command Authorization Set for a User, page 7-29
  - Configuring Device-Management Command Authorization for a User, page 7-30
  - Configuring the Unknown Service Setting for a User, page 7-32
- Advanced TACACS+ Settings (User), page 7-33
  - Setting Enable Privilege Options for a User, page 7-33
  - Setting TACACS+ Enable Password Options for a User, page 7-35
  - Setting TACACS+ Outbound Password for a User, page 7-37




Downloaded from www.Manualslib.com manuals search engine

- RADIUS Attributes, page 7-37
  - Setting IETF RADIUS Parameters for a User, page 7-38
  - Setting Cisco IOS/PIX RADIUS Parameters for a User, page 7-39
  - Setting Cisco Aironet RADIUS Parameters for a User, page 7-41
  - Setting Ascend RADIUS Parameters for a User, page 7-43
  - Setting Cisco VPN 3000 Concentrator RADIUS Parameters for a User, page 7-44
  - Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User, page 7-46
  - Setting Microsoft RADIUS Parameters for a User, page 7-47
  - Setting Nortel RADIUS Parameters for a User, page 7-49
  - Setting Juniper RADIUS Parameters for a User, page 7-51
  - Setting BBSM RADIUS Parameters for a User, page 7-52
  - Setting Custom RADIUS Attributes for a User, page 7-53

# TACACS+ Settings (User)

The TACACS+ Settings section permits you to enable and configure the service/protocol parameters to be applied for the authorization of a user.

This section contains the following topics:

- Configuring TACACS+ Settings for a User, page 7-24
- Configuring a Shell Command Authorization Set for a User, page 7-26
- Configuring a PIX Command Authorization Set for a User, page 7-29
- Configuring Device-Management Command Authorization for a User, page 7-30
- Configuring the Unknown Service Setting for a User, page 7-32



Downloaded from www.Manualslib.com manuals search engine

## Configuring TACACS+ Settings for a User

You can use this procedure to configure TACACS+ settings at the user level for the following service/protocols:

- PPP IP
- PPP IPX
- PPP Multilink
- PPP Apple Talk
- PPP VPDN
- PPP LCP
- ARAP
- Shell (exec)
- PIX Shell (pixShell)
- SLIP

You can also enable any *new* TACACS+ services that you may have configured. Because having all service/protocol settings display within the User Setup section would be cumbersome, you choose what settings to hide or display at the user level when you configure the interface. For more information about setting up new or existing TACACS+ services in the Cisco Secure ACS HTML interface, see Protocol Configuration Options for TACACS+, page 3-7.

If you have configured Cisco Secure ACS to interact with a Cisco device-management application, new TACACS+ services may appear automatically, as needed to support the device-management application. For more information about Cisco Secure ACS interaction with device-management applications, see Support for Cisco Device-Management Applications, page 1-19.

For more information about attributes, see Appendix B, "TACACS+ Attribute-Value Pairs", or your AAA client documentation. For information on assigning an IP ACL, see Assigning a Downloadable IP ACL to a User, page 7-21.



Downloaded from www.Manualslib.com manuals search engine

### Before You Begin

- For the TACACS+ service/protocol configuration to be displayed, a AAA client must be configured to use TACACS+ as the security control protocol.
- In the Advanced Options section of Interface Configuration, ensure that the Per-user TACACS+/RADIUS Attributes check box is selected.

To configure TACACS+ settings for a user, follow these steps:

**Step 1** Click **Interface Configuration** and then click **TACACS+ (Cisco IOS)**. In the TACACS+ Services table, under the heading User, ensure that the check box is selected for each service/protocol you want to configure.

**Step 2** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 3** Scroll down to the TACACS+ Settings table and select the bold service name check box to enable that protocol; for example (PPP IP).

**Step 4** To enable specific parameters within the selected service, select the check box next to a specific parameter and then do one of the following, as applicable:

- Select the **Enabled** check box.
- Specify a value in the corresponding attribute box.

  To specify ACLs and IP address pools, enter the name of the ACL or pool as defined on the AAA client. Leave the box blank if the default (as defined on the AAA client) should be used. For more information about attributes, see Appendix B, "TACACS+ Attribute-Value Pairs", or your AAA client documentation. For information on assigning a IP ACL, see Assigning a Downloadable IP ACL to a User, page 7-21.

**Tip** An ACL is a list of Cisco IOS commands used to restrict access to or from other devices and users on the network.

**Step 5** To employ custom attributes for a particular service, select the **Custom attributes** check box under that service, and then specify the attribute/value in the box below the check box.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

## Configuring a Shell Command Authorization Set for a User

Use this procedure to specify the shell command authorization set parameters for a user. You can choose one of five options:

- **None**—There is no authorization for shell commands.
- **Group**—For this user, the group-level shell command authorization set applies.
- **Assign a Shell Command Authorization Set for any network device**—One shell command authorization set is assigned, and it applies all network devices.
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Particular shell command authorization sets are to be effective on particular NDGs. When you select this option, you create the table that lists what NDG associates with what shell command authorization set.
- **Per User Command Authorization**—Enables you to permit or deny specific Cisco IOS commands and arguments at the user level.

**Before You Begin**

- Make sure that a AAA client has been configured to use TACACS+ as the security control protocol.
- In the Advanced Options section of Interface Configuration, ensure that the Per-user TACACS+/RADIUS Attributes check box is selected.
- In the TACACS+ (Cisco) section of Interface Configuration, ensure that the Shell (exec) option is selected in the User column.
- Ensure that you have already configured one or more shell command authorization sets. For detailed steps, see Adding a Command Authorization Set, page 5-31.



Downloaded from www.Manualslib.com manuals search engine

To specify shell command authorization set parameters for a user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Scroll down to the TACACS+ Settings table and to the Shell Command Authorization Set feature area within it.

**Step 3** To prevent the application of any shell command authorization set, select (or accept the default of) the **None** option.

**Step 4** To assign the shell command authorization set at the group level, select the **As Group** option.

**Step 5** To assign a particular shell command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a Shell Command Authorization Set for any network device** option.

b. Then, from the list directly below that option, select the shell command authorization set you want applied to this user.

**Step 6** To create associations that assign a particular shell command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

**Tip** You can also select which command set applies to network device groups that are not listed simply by associating that command set with the NDG <*default*> listing.

The NDG or NDGs and associated shell command authorization set or sets are paired in the table.



Downloaded from www.Manualslib.com manuals search engine

**Step 7** To define the specific Cisco IOS commands and arguments to be permitted or denied for this user, follow these steps:

a. Select the **Per User Command Authorization** option.

b. Under Unmatched Cisco IOS commands, select either **Permit** or **Deny**.

If you select Permit, the user can issue all commands not specifically listed. If you select Deny, the user can issue only those commands listed.

c. To list particular commands to be permitted or denied, select the **Command** check box and then type the name of the command, define its arguments using standard permit or deny syntax, and select whether unlisted arguments are to be permitted or denied.

**Caution** This is a powerful, advanced feature and should be used by an administrator skilled with Cisco IOS commands. Correct syntax is the responsibility of the administrator. For information on how Cisco Secure ACS uses pattern matching in command arguments, see About Pattern Matching, page 5-30.

**Tip** To enter several commands, you must click **Submit** after specifying a command. A new command entry box appears below the box you just completed.

**Step 8** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

## Configuring a PIX Command Authorization Set for a User

Use this procedure to specify the PIX command authorization set parameters for a user. There are four options:

- **None**—No authorization for PIX commands.
- **Group**—For this user, the group-level PIX command authorization set applies.
- **Assign a PIX Command Authorization Set for any network device**—One PIX command authorization set is assigned, and it applies to all network devices.
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command authorization sets are to be effective on particular NDGs.

**Before You Begin**

- Make sure that a AAA client is configured to use TACACS+ as the security control protocol.
- In the Advanced Options section of Interface Configuration, make sure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In the TACACS+ (Cisco) section of Interface Configuration, make sure that the **PIX Shell (pixShell)** option is selected in the User column.
- Make sure that you have configured one or more PIX command authorization sets. For detailed steps, see Adding a Command Authorization Set, page 5-31.

To specify PIX command authorization set parameters for a user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Scroll down to the TACACS+ Settings table and to the PIX Command Authorization Set feature area within it.

**Step 3** To prevent the application of any PIX command authorization set, select (or accept the default of) the **None** option.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** To assign the PIX command authorization set at the group level, select the **As Group** option.

**Step 5** To assign a particular PIX command authorization set to be effective on any configured network device, follow these steps:

a. Select the **Assign a PIX Command Authorization Set for any network device** option.

b. From the list directly below that option, select the PIX command authorization set you want applied to this user.

**Step 6** To create associations that assign a particular PIX command authorization set to be effective on a particular NDG, for each association, follow these steps:

a. Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.

b. Select a **Device Group** and an associated **Command Set**.

c. Click **Add Association**.

The associated NDG and PIX command authorization set appear in the table.

**Step 7** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

## Configuring Device-Management Command Authorization for a User

Use this procedure to specify the device-management command authorization set parameters for a user. Device-management command authorization sets support the authorization of tasks in Cisco device-management applications that are configured to use Cisco Secure ACS for authorization. You can choose one of four options:

- **None**—No authorization is performed for commands issued in the applicable Cisco device-management application.
- **Group**—For this user, the group-level command authorization set applies for the applicable device-management application.



Downloaded from www.Manualslib.com manuals search engine

- **Assign a** *device-management application* for any network device—For the applicable device-management application, one command authorization set is assigned, and it applies to management tasks on all network devices.
- **Assign a** *device-management application* on a per Network Device Group Basis—For the applicable device-management application, this option enables you to apply command authorization sets to specific NDGs, so that it affects all management tasks on the network devices belonging to the NDG.

**Before You Begin**

- Make sure that a AAA client is configured to use TACACS+ as the security control protocol.
- In the Advanced Options section of Interface Configuration, make sure that the Per-user TACACS+/RADIUS Attributes check box is selected.
- In the TACACS+ (Cisco) section of Interface Configuration, make sure that, under New Services, the new TACACS+ service corresponding to the applicable device-management application is selected in the User column.
- If you want to apply command authorization sets, make sure that you have configured one or more device management command authorization sets. For detailed steps, see Adding a Command Authorization Set, page 5-31.

To specify device-management application command authorization for a user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Scroll down to the TACACS+ Settings table and to the applicable device-management command authorization feature area within it.

**Step 3** To prevent the application of any command authorization for actions performed in the applicable device-management application, select (or accept the default of) the **None** option.

**Step 4** To assign command authorization for the applicable device-management application at the group level, select the **As Group** option.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** To assign a particular command authorization set that affects device-management application actions on any network device, follow these steps:

a. Select the **Assign a** *device-management application* for any network device option.

b. Then, from the list directly below that option, select the command authorization set you want applied to this user.

**Step 6** To create associations that assign a particular command authorization set that affects device-management application actions on a particular NDG, for each association, follow these steps:

a. Select the **Assign a** *device-management application* on a per Network Device Group Basis option.

b. Select a **Device Group** and an associated *device-management application*.

c. Click **Add Association**.

The associated NDG and command authorization set appear in the table.

**Step 7** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

## Configuring the Unknown Service Setting for a User

If you want TACACS+ AAA clients to permit unknown services, you can select the Default (Undefined) Services check box under Checking this option will PERMIT all UNKNOWN Services.

To configure the Unknown Service setting for a user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Scroll down to the table under the heading Checking this option will PERMIT all UNKNOWN Services.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** To allow TACACS+ AAA clients to permit unknown services for this user, select the **Default (Undefined) Services** check box.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

# Advanced TACACS+ Settings (User)

The information presented in this section applies when you have a AAA client with TACACS+ configured.

**Tip** If the Advanced TACACS+ Settings (User) table does not appear, click **Interface Configuration**, click **TACACS+ (Cisco IOS)**, and then click **Advanced TACACS+ Features**.

This section contains the following topics:

- Setting Enable Privilege Options for a User, page 7-33
- Setting TACACS+ Enable Password Options for a User, page 7-35
- Setting TACACS+ Outbound Password for a User, page 7-37

## Setting Enable Privilege Options for a User

You use TACACS+ Enable Control with Exec session to control administrator access. Typically, you use it for router management control. From the following four options, you can select and specify the privilege level you want a user to have.

- **Use Group Level Setting**—Sets the privileges for this user as those configured at the group level.
- **No Enable Privilege**—Disallows enable privileges for this user.



Downloaded from www.Manualslib.com manuals search engine

**Note** This is the default setting.

- **Max Privilege for any AAA Client**—Enables you to select from a list the maximum privilege level that will apply to this user on any AAA client on which this user is authorized.
- **Define Max Privilege on a per-Network Device Group Basis**—Enables you to associate maximum privilege levels to this user in one or more NDGs.

**Note** For information about privilege levels, refer to your AAA client documentation.

**Tip** You must configure NDGs from within Interface Configuration before you can assign user privilege levels to them.

To select and specify the privilege level for a user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Under TACACS+ Enable Control in the Advanced TACACS+ Settings table, select one of the four privilege options, as follows:

- Use Group Level Setting
- No Enable Privilege

**Note** (No Enable Privilege is the default setting; when setting up an new user account, it should already be selected.)

- Max Privilege for Any Access Server
- Define Max Privilege on a per-Network Device Group Basis

**Step 3** If you selected Max Privilege for Any Access Server in Step 2, select the appropriate privilege level from the corresponding list.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** If you selected Define Max Privilege on a per-Network Device Group Basis in Step 2, perform the following steps to define the privilege levels on each NDG, as applicable:

**a.** From the Device Group list, select a device group.

**Note** You must have already configured a device group for it to be listed.

**b.** From the Privilege list, select a privilege level to associate with the selected device group.

**c.** Click **Add Association**.

An entry appears in the table, associating the device group with a particular privilege level.

**d.** Repeat Step a through Step c for each device group you want to associate to this user.

**Tip** To delete an entry, select the entry and then click **Remove Associate**.

**Step 5** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

## Setting TACACS+ Enable Password Options for a User

When setting the TACACS+ Enable Password Options for a user, you have three options to chose from:

- Use CiscoSecure PAP password.
- Use external database password.
- Use separate password.



Downloaded from www.Manualslib.com manuals search engine

To set the options for the TACACS+ Enable password, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Do one of the following:

- To use the information configured in the Password Authentication section, select **Use CiscoSecure PAP password**.

  **Note** For information about basic password setup, see Adding a Basic User Account, page 7-4.

- To use an external database password, select **Use external database password**, and then choose from the list the database that authenticates the enable password for this user.

  **Note** The list of databases displays only the databases that you have configured. For more information, see About External User Databases, page 13-4.

- To use a separate password, click **Use separate password**, and then type and retype to confirm a control password for this user. This password is used in addition to the regular authentication.

**Step 3** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

## Setting TACACS+ Outbound Password for a User

The TACACS+ outbound password enables a AAA client to authenticate itself to another AAA client via outbound authentication. The outbound authentication can be PAP, CHAP, MS-CHAP, or ARAP, and results in the Cisco Secure ACS password being given out. By default, the user ASCII/PAP or CHAP/MS-CHAP/ARAP password is used. To prevent compromising inbound passwords, you can configure a separate SENDAUTH password.

**Caution** Use an outbound password only if you are familiar with the use of a TACACS+ SendAuth/OutBound password.

To set a TACACS+ outbound password for a user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Type and retype to confirm a TACACS+ outbound password for this user.

**Step 3** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

# RADIUS Attributes

You can configure user attributes for RADIUS authentication either generally, at the IETF level, or for vendor-specific attributes (VSAs) on a vendor-by-vendor basis. For general attributes, see Setting IETF RADIUS Parameters for a User, page 7-38. Cisco Secure ACS ships with many popular VSAs already loaded and available to configure and apply. For information about creating additional, custom RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-28.



Downloaded from www.Manualslib.com manuals search engine

This section contains the following topics:


- Setting IETF RADIUS Parameters for a User, page 7-38
- Setting Cisco IOS/PIX RADIUS Parameters for a User, page 7-39
- Setting Cisco Aironet RADIUS Parameters for a User, page 7-41
- Setting Ascend RADIUS Parameters for a User, page 7-43
- Setting Cisco VPN 3000 Concentrator RADIUS Parameters for a User, page 7-44
- Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User, page 7-46
- Setting Microsoft RADIUS Parameters for a User, page 7-47
- Setting Nortel RADIUS Parameters for a User, page 7-49
- Setting Juniper RADIUS Parameters for a User, page 7-51
- Setting BBSM RADIUS Parameters for a User, page 7-52
- Setting Custom RADIUS Attributes for a User, page 7-53


## Setting IETF RADIUS Parameters for a User

RADIUS attributes are sent as a profile for the user from Cisco Secure ACS to the requesting AAA client.

These parameters display only if all the following are true:

- A AAA client is configured to use one of the RADIUS protocols in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level IETF RADIUS attributes are enabled under RADIUS (IETF) in the Interface Configuration section.

**Note** To display or hide any of these attributes in the HTML interface, see Protocol Configuration Options for RADIUS, page 3-11.



Downloaded from www.Manualslib.com manuals search engine

**Note** For a list and explanation of RADIUS attributes, see Appendix C, "RADIUS Attributes", or the documentation for your particular network device using RADIUS.

To configure IETF RADIUS attribute settings to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** In the IETF RADIUS table, for each attribute that you need to authorize for the current user, select the check box next to the attribute and then further define the authorization for the attribute in the box or boxes next to it, as applicable.

**Step 3** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

## Setting Cisco IOS/PIX RADIUS Parameters for a User

The Cisco IOS RADIUS parameters appear only if all the following are true:

- A AAA client is configured to use RADIUS (Cisco IOS/PIX) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Cisco IOS/PIX) attributes are enabled under RADIUS (Cisco IOS/PIX) in the Interface Configuration section.

**Note** To hide or display the Cisco IOS RADIUS VSA, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular user persists, even when you remove or



Downloaded from www.Manualslib.com manuals search engine

replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

Cisco IOS RADIUS represents only the Cisco IOS VSAs. You must configure both the IETF RADIUS and Cisco IOS RADIUS attributes.

To configure and enable Cisco IOS RADIUS attributes to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Before configuring Cisco IOS RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-38.

**Step 3** If you want to use the [009\001] cisco-av-pair attribute to specify authorizations, select the check box next to the attribute and then type the attribute-value pairs in the text box. Separate each attribute-value pair by pressing Enter.

For example, if the current user profile corresponds to a Network Admission Control (NAC) client to which Cisco Secure ACS always assigns a status-query-timeout attribute value that needs to be different than a value that any applicable group profile contains, you could specify that value as follows:

```
status-query-timeout=1200
```

**Step 4** If you want to use other Cisco IOS/PIX RADIUS attributes, select the corresponding check box and specify the required values in the adjacent text box.

**Step 5** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

## Setting Cisco Aironet RADIUS Parameters for a User

The single Cisco Aironet RADIUS VSA, Cisco-Aironet-Session-Timeout, is a virtual VSA. It acts as a specialized implementation (that is, a remapping) of the IETF RADIUS Session-Timeout attribute (27) to respond to a request from a Cisco Aironet Access Point. You use it to provide a different timeout values when a user must be able to connect via both wireless and wired devices. This capability to provide a second timeout value specifically for WLAN connections avoids the difficulties that would arise if you had to use a standard timeout value (typically measured in hours) for a WLAN connection (that is typically measured in minutes). You do not need to use Cisco-Aironet-Session-Timeout if the particular user will always connect only with a Cisco Aironet Access Point. Rather, use this setting when a user may connect via wired or wireless clients.

For example, imagine a user's Cisco-Aironet-Session-Timeout set to 600 seconds (10 minutes) and that same user's IETF RADIUS Session-Timeout set to 3 hours. When the user connects via a VPN, Cisco Secure ACS uses 3 hours as the timeout value. However, if that same user connects via a Cisco Aironet Access Point, Cisco Secure ACS responds to an authentication request from the Aironet AP by sending 600 seconds in the IETF RADIUS Session-Timeout attribute. Thus, with the Cisco-Aironet-Session-Timeout attribute configured, different session timeout values can be sent depending on whether the end-user client is a wired device or a Cisco Aironet Access Point.

The Cisco Aironet RADIUS parameters appear on the User Setup page only if all the following are true:

- A AAA client is configured to use RADIUS (Cisco Aironet) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Cisco Aironet) attribute is enabled under RADIUS (Cisco Aironet) in the Interface Configuration section.

**Note** To hide or display the Cisco Aironet RADIUS VSA, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.



Downloaded from www.Manualslib.com manuals search engine

To configure and enable the Cisco Aironet RADIUS attribute to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Before configuring Cisco Aironet RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-38.

**Step 3** In the Cisco Aironet RADIUS Attributes table, select the **[5842\001] Cisco-Aironet-Session-Timeout** check box.

**Step 4** In the [5842\001] Cisco-Aironet-Session-Timeout box, type the session timeout value (in seconds) that Cisco Secure ACS is to send in the IETF RADIUS Session-Timeout (27) attribute when the AAA client is configured in Network Configuration to use the RADIUS (Cisco Aironet) authentication option. The recommended value is 600 seconds.

For more information about the IETF RADIUS Session-Timeout attribute, see Appendix C, "RADIUS Attributes", or your AAA client documentation.

**Step 5** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

## Setting Ascend RADIUS Parameters for a User

The Ascend RADIUS parameters appear only if all the following are true:

- A AAA client is configured to use RADIUS (Ascend) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Ascend) attributes you want to apply are enabled under RADIUS (Ascend) in the Interface Configuration section.

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure both the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting displayed for RADIUS is `Ascend-Remote-Addr`.

**Note** To hide or display Ascend RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Ascend RADIUS attributes to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Before configuring Ascend RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-38.

**Step 3** In the Ascend RADIUS Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

**a.** Select the check box next to the particular attribute.

**b.** Further define the authorization for that attribute in the box next to it.

**c.** Continue to select and define attributes, as applicable.



Downloaded from www.Manualslib.com manuals search engine

For more information about attributes, see Appendix C, "RADIUS Attributes", or your AAA client documentation.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

## Setting Cisco VPN 3000 Concentrator RADIUS Parameters for a User

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, Cisco Secure ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the Cisco Secure ACS HTML interface or how those attributes might be configured.

The Cisco VPN 3000 Concentrator RADIUS attribute configurations appear only if all the following are true:

- A AAA client is configured to use RADIUS (Cisco VPN 3000) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Cisco VPN 3000) attributes you want to apply are enabled under RADIUS (Cisco VPN 3000) in the Interface Configuration section.

Cisco VPN 3000 Concentrator RADIUS represents only the Cisco VPN 3000 Concentrator VSA. You must configure both the IETF RADIUS and Cisco VPN 3000 Concentrator RADIUS attributes.



Downloaded from www.Manualslib.com manuals search engine

**Note** To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco VPN 3000 Concentrator RADIUS attributes to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Before configuring Cisco VPN 3000 Concentrator RADIUS attributes, be sure your IETF RADIUS attributes are configured properly.

For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-38.

**Step 3** In the Cisco VPN 3000 Concentrator Attribute table, to specify the attributes that should be authorized for the user, follow these steps:

**a.** Select the check box next to the particular attribute.

**b.** Further define the authorization for that attribute in the box next to it.

**c.** Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes", or your AAA client documentation.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

# Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User

The Cisco VPN 5000 Concentrator RADIUS attribute configurations display only if all the following are true:

- A AAA client is configured to use RADIUS (Cisco VPN 5000) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Cisco VPN 5000) attributes you want to apply are enabled under RADIUS (Cisco VPN 5000) in the Interface Configuration section.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSA. You must configure both the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.

**Note** To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Before configuring Cisco VPN 5000 Concentrator RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-38.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** In the Cisco VPN 5000 Concentrator Attribute table, to specify the attributes that should be authorized for the user, follow these steps:

a. Select the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes", or your AAA client documentation.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

## Setting Microsoft RADIUS Parameters for a User

Microsoft RADIUS provides VSAs supporting Microsoft Point-to-Point Encryption (MPPE), which is an encryption technology developed by Microsoft to encrypt point-to-point (PPP) links. These PPP connections can be via a dial-in line, or over a Virtual Private Network (VPN) tunnel.

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, Cisco Secure ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the Cisco Secure ACS HTML interface or how those attributes might be configured.



Downloaded from www.Manualslib.com manuals search engine

The Microsoft RADIUS attribute configurations display only if both the following are true:

- A AAA client is configured in Network Configuration that uses a RADIUS protocol that supports the Microsoft RADIUS VSA.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- The user-level RADIUS (Microsoft) attributes you want to apply are enabled under RADIUS (Microsoft) in the Interface Configuration section.

The following Cisco Secure ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS
- Cisco VPN 3000
- Cisco VPN 5000
- Ascend

Microsoft RADIUS represents only the Microsoft VSA. You must configure both the IETF RADIUS and Microsoft RADIUS attributes.

**Note** To hide or display Microsoft RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Microsoft RADIUS attributes to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Before configuring Cisco IOS RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-38.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** In the Microsoft RADIUS Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

a. Select the check box next to the particular attribute.

b. Further define the authorization for that attribute in the box next to it.

c. Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes", or your AAA client documentation.

**Note** The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

## Setting Nortel RADIUS Parameters for a User

The Nortel RADIUS parameters appear only if all the following are true:

- A AAA client is configured to use RADIUS (Nortel) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Nortel) attributes you want to apply are enabled under RADIUS (Nortel) in the Interface Configuration section.

Nortel RADIUS represents only the Nortel proprietary attributes. You must configure both the IETF RADIUS and Nortel RADIUS attributes. Proprietary attributes override IETF attributes.



Downloaded from www.Manualslib.com manuals search engine

**Note** To hide or display Nortel RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Nortel RADIUS attributes to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Before configuring Nortel RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-38.

**Step 3** In the Nortel RADIUS Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

**a.** Select the check box next to the particular attribute.

**b.** Further define the authorization for that attribute in the box next to it.

**c.** Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes", or your AAA client documentation.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.



Downloaded from www.Manualslib.com manuals search engine

## Setting Juniper RADIUS Parameters for a User

The Juniper RADIUS parameters appear only if all the following are true:

- A AAA client is configured to use RADIUS (Juniper) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (Juniper) attributes you want to apply are enabled under RADIUS (Juniper) in the Interface Configuration section.

Juniper RADIUS represents only the Juniper proprietary attributes. You must configure both the IETF RADIUS and Juniper RADIUS attributes. Proprietary attributes override IETF attributes.

**Note** To hide or display Juniper RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Juniper RADIUS attributes to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Before configuring Juniper RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-38.

**Step 3** In the Juniper RADIUS Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

**a.** Select the check box next to the particular attribute.

**b.** Further define the authorization for that attribute in the box next to it.

**c.** Continue to select and define attributes, as applicable.



Downloaded from www.Manualslib.com manuals search engine

For more information about attributes, see Appendix C, "RADIUS Attributes", or your AAA client documentation.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

## Setting BBSM RADIUS Parameters for a User

The BBSM RADIUS parameters appear only if all the following are true:

- A AAA client is configured to use RADIUS (BBSM) in Network Configuration.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (BBSM) attributes you want to apply are enabled under RADIUS (BBSM) in the Interface Configuration section.

BBSM RADIUS represents only the BBSM proprietary attributes. You must configure both the IETF RADIUS and BBSM RADIUS attributes. Proprietary attributes override IETF attributes.

**Note** To hide or display BBSM RADIUS attributes, see Setting Protocol Configuration Options for Non-IETF RADIUS Attributes, page 3-17. A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable BBSM RADIUS attributes to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Before configuring BBSM RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-38.

**Step 3** In the BBSM RADIUS Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

**a.** Select the check box next to the particular attribute.

**b.** Further define the authorization for that attribute in the box next to it.

**c.** Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes", or your AAA client documentation.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

## Setting Custom RADIUS Attributes for a User

Custom RADIUS parameters appear only if all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see Custom RADIUS Vendors and VSAs, page 9-28.)
- A AAA client is configured in Network Configuration that uses a RADIUS protocol that supports the custom VSA.
- The Per-user TACACS+/RADIUS Attributes check box is selected under Advanced Options in the Interface Configuration section.
- User-level RADIUS (*custom name*) attributes you want to apply are enabled under RADIUS (*custom name*) in the Interface Configuration section.

You must configure both the IETF RADIUS and the custom RADIUS attributes. Proprietary attributes override IETF attributes.



Downloaded from www.Manualslib.com manuals search engine

To configure and enable custom RADIUS attributes to be applied as an authorization for the current user, follow these steps:

**Step 1** Perform Step 1 through Step 3 of Adding a Basic User Account, page 7-4.

The User Setup Edit page opens. The username being added or edited is at the top of the page.

**Step 2** Before configuring custom RADIUS attributes, be sure your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see Setting IETF RADIUS Parameters for a User, page 7-38.

**Step 3** In the RADIUS *custom name* Attributes table, to specify the attributes that should be authorized for the user, follow these steps:

**a.** Select the check box next to the particular attribute.

**b.** Further define the authorization for that attribute in the box next to it, as required.

**c.** Continue to select and define attributes, as applicable.

For more information about attributes, see Appendix C, "RADIUS Attributes", or your AAA client documentation.

**Step 4** Do one of the following:

- If you are finished configuring the user account options, click **Submit** to record the options.
- To continue to specify the user account options, perform other procedures in this chapter, as applicable.

# User Management

This section describes how to use the User Setup section to perform a variety of user account managerial tasks.

This section contains the following topics:

- Listing All Users, page 7-55
- Finding a User, page 7-55
- Disabling a User Account, page 7-56



Downloaded from www.Manualslib.com manuals search engine

- Deleting a User Account, page 7-57
- Resetting User Session Quota Counters, page 7-58
- Resetting a User Account after Login Failure, page 7-59
- Saving User Settings, page 7-60

# Listing All Users

The User List displays all user accounts (enabled and disabled). The list includes, for each user, the username, status, and the group to which the user belongs.

Usernames are displayed in the order in which they were entered into the database. This list cannot be sorted.

To view a list of all user accounts, follow these steps:

**Step 1** In the navigation bar, click **User Setup**.

The User Setup Select page opens.

**Step 2** Click **List All Users**.

In the display area on the right, the User List appears.

**Step 3** To view or edit the information for an individual user, click the username in the right window.

The user account information appears.

# Finding a User

To find a user, follow these steps:

**Step 1** In the navigation bar, click **User Setup**.

The User Setup Select page opens.

**Step 2** Type the name in the **User** box, and then click **Find**.



Downloaded from www.Manualslib.com manuals search engine

**Tip** You can use wildcard characters (*) in this box.

**Tip** To display a list of usernames that begin with a particular letter or number, click the letter or number in the alphanumeric list. A list of users whose names begin with that letter or number opens in the display area on the right.

The username, status (enabled or disabled), and group to which the user belongs appear in the display area on the right.

**Step 3** To view or edit the information for the user, click the username in the display area on the right.

The user account information appears.

# Disabling a User Account

This procedure details how to manually disable a user account in the CiscoSecure user database.

**Note** To configure the conditions by which a user account will automatically be disabled, see Setting Options for User Account Disablement, page 7-20.

**Note** This is not to be confused with account expiration due to password aging. Password aging is defined for groups only, not for individual users.

To disable a user account, follow these steps:

**Step 1** In the navigation bar, click **User Setup**.

The User Setup Select page opens.

**Step 2** In the **User** box, type the name of the user whose account is to be disabled.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** Click **Add/Edit**.

The User Setup Edit page opens. The username being edited is at the top of the page.

**Step 4** Select the **Account Disabled** check box.

**Step 5** Click **Submit** at the bottom of the page.

The specified user account is disabled.

# Deleting a User Account

You can delete user accounts one at a time using the HTML interface.

**Note** If you are authenticating using the Unknown User policy and you want deny a user access by deleting the user account, you must also delete the user account from the external user database. This prevents the username from being automatically re-added to the CiscoSecure user database the next time the user attempts to log in.

**Tip** For deleting batches of user accounts, use the RDBMS Synchronization feature with action code 101 (see RDBMS Synchronization, page 9-25, for more information.).

To delete a user account, follow these steps:

**Step 1** Click **User Setup**.

The User Setup Select page of the HTML interface opens.

**Step 2** In the **User** box, type the complete username to be deleted.

**Note** Alternatively, you can click **List All Users** and then select the user from the list that appears.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** Click **Add/Edit**.

**Step 4** At the bottom of the User Setup page, click **Delete**.

**Note** The Delete button appears only when you are editing user information, not when you are adding a username.

A popup window appears that asks you to confirm the user deletion.

**Step 5** Click **OK**.

The user account is removed from the CiscoSecure user database.

# Resetting User Session Quota Counters

You can reset the session quota counters for a user either before or after the user exceeds a quota.

To reset user usage quota counters, follow these steps:

**Step 1** Click **User Setup**.

The Select page of the HTML interface opens.

**Step 2** In the User box, type the complete username of the user whose session quota counters you are going to reset.

**Note** Alternatively, you can click **List All Users** and then select the user from the list that appears.

**Step 3** Click **Add/Edit**.

**Step 4** In the Session Quotas section, select the **Reset All Counters on submit** check box.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** Click **Submit** at the bottom of the browser page.

The session quota counters are reset for this user. The User Setup Select page appears.

# Resetting a User Account after Login Failure

Perform this procedure when an account is disabled because the failed attempts count has been exceeded during an unsuccessful user attempt to log in.

To reset a user account after login failure, follow these steps:

**Step 1** Click **User Setup**.

The User Setup Select page of the HTML interface opens.

**Step 2** In the **User** box, type the complete username of the account to be reset.

**Note** Alternatively, you can click List All Users and then select the user from the list that appears.

**Step 3** Click **Add/Edit**.

**Step 4** In the Account Disable table, select the **Reset current failed attempts count on submit** check box, and then click **Submit**.

The Failed attempts since last successful login: counter resets to 0 (zero) and the system re-enables the account.

**Note** This counter shows the number of unsuccessful login attempts since the last time this user logged in successfully.



Downloaded from www.Manualslib.com manuals search engine

**Note** If the user authenticates with a Windows user database, this expiration information is in addition to the information in the Windows user account. Changes here do not alter settings configured in Windows.

# Saving User Settings

After you have completed configuration for a user, be sure to save your work.

To save the configuration for the current user, follow these steps:

**Step 1** To save the user account configuration, click **Submit**.

**Step 2** To verify that your changes were applied, type the username in the **User** box and click **Add/Edit**, and then review the settings.



Downloaded from www.Manualslib.com manuals search engine

# System Configuration: Basic

This chapter addresses the basic features found in the System Configuration section of Cisco Secure ACS for Windows Server.

This chapter contains the following topics:


- Service Control, page 8-1
- Logging, page 8-3
- Date Format Control, page 8-3
- Local Password Management, page 8-5
- Cisco Secure ACS Backup, page 8-9
- Cisco Secure ACS System Restore, page 8-14
- Cisco Secure ACS Active Service Management, page 8-17
- VoIP Accounting Configuration, page 8-21


## Service Control

Cisco Secure ACS uses several services. The Service Control page provides basic status information about the services, and enables you to configure the service log files and to stop or restart the services. For more information about Cisco Secure ACS services, see Chapter 1, “Overview”.



Downloaded from www.Manualslib.com manuals search engine

**Tip** You can configure Cisco Secure ACS service logs. For more information, see Configuring Service Logs, page 11-33.

This section contains the following topics:


- Determining the Status of Cisco Secure ACS Services, page 8-2
- Stopping, Starting, or Restarting Services, page 8-2


# Determining the Status of Cisco Secure ACS Services

You can determine whether Cisco Secure ACS services are running or stopped by accessing the Service Control page.

To determine the status of Cisco Secure ACS services, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Service Control**.

The status of the services appears in the CiscoSecure ACS on *hostname* table, where *hostname* is the name of the Cisco Secure ACS.

# Stopping, Starting, or Restarting Services

You can stop, start, or restart Cisco Secure ACS services as needed. This achieves the same result as starting and stopping Cisco Secure ACS services from within Windows Control panel. This procedure stops, starts, or restarts the Cisco Secure ACS services except for CSAdmin, which is responsible for the HTML interface.

**Note** If the CSAdmin service needs to be restarted, you can do so using the Control Panel Services applet; however, it is best to allow Cisco Secure ACS to handle the services because there are dependencies in the order in which the services are started.

To stop, start, or restart Cisco Secure ACS services, follow these steps:



Downloaded from www.Manualslib.com manuals search engine

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Service Control**.

The status of the services appears in the CiscoSecure ACS on *hostname* table, where *hostname* is the name of the Cisco Secure ACS.

If the services are running, the Restart and Stop buttons appear at the bottom of the page.

If the services are stopped, the Start button appears at the bottom of the page.

**Step 3** Click **Stop**, **Start**, or **Restart**, as applicable.

The status of Cisco Secure ACS services changes to the state appropriate to the button you clicked.

# Logging

You can configure Cisco Secure ACS to generate logs for administrative and accounting events, depending on the protocols and options you have enabled. For more information, including configuration steps, see Chapter 1, "Overview".

# Date Format Control

Cisco Secure ACS allows for one of two possible date formats in its logs, reports, and administrative interface. You can choose either a month/day/year format or a day/month/year format.

## Setting the Date Format

**Note** If you have reports that were generated before you changed the date format, be sure to move or rename them to avoid conflicts. For example, if you are using the month/day/year format, Cisco Secure ACS assigns the name 2001-07-12.csv to a



Downloaded from www.Manualslib.com manuals search engine

report generated on July 12, 2001. If you subsequently change to the day/month/year format, on December 7, 2001, Cisco Secure ACS creates a file also named 2001-07-12.csv and overwrites the existing file.

To set the date format, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Date Format Control**.

Cisco Secure ACS displays the Date Format Selection table.

**Step 3** Select a date format option.

**Step 4** Click **Submit & Restart**.

Cisco Secure ACS restarts its services and implements the date format you selected.

**Note** For the new date format to be seen in the HTML interface reports, you must restart the connection to the Cisco Secure ACS. Click the **Logoff** button (a button with an X) in the upper-right corner of the browser window.



Downloaded from www.Manualslib.com manuals search engine

# Local Password Management

You use the Local Password Management page to configure settings that apply to managing passwords stored in the CiscoSecure user database. It contains the following three sections:

- **Password Validation Options**—These settings enable you to configure validation parameters for user passwords. Cisco Secure ACS enforces these rules when an administrator changes a user password in the CiscoSecure user database and when a user attempts to change passwords using the CiscoSecure Authentication Agent applet.

  **Note** Password validation options apply only to user passwords stored in the CiscoSecure user database. They do not apply to passwords in user records kept in external user databases nor do they apply to enable or admin passwords for Cisco IOS network devices.

  The password validation options are listed below:

  - **Password length between *X* and *Y* characters**—Enforces that password lengths be between the values specified in the *X* and *Y* boxes, inclusive. Cisco Secure ACS supports passwords up to 32 characters long.
  - **Password may not contain the username**—Requires that a user password does not contain the username anywhere within it.
  - **Password is different from the previous value**—Requires a new user password to be different from the previous password.
  - **Password must be alphanumeric**—Requires a user password to contain both letters and numbers.

- **Remote Change Password**—These settings enable you to configure whether Telnet password change is enabled and, if it is enabled, whether Cisco Secure ACS immediately sends the updated user data to its replication partners.

  The remote change password options are listed below:

  - **Disable TELNET Change Password against this ACS and return the following message to the users telnet session**—When selected, this option disables the ability to perform password changes during a Telnet session hosted by a TACACS+ AAA client. Users who submit a password change receive the text message that you type in the corresponding box.



Downloaded from www.Manualslib.com manuals search engine

- **Upon remote user password change, immediately propagate the change to selected replication partners**—This setting determines whether Cisco Secure ACS sends to its replication partners any passwords changed during a Telnet session hosted by a TACACS+ AAA client, by the CiscoSecure Authentication Agent, or by the User-Changeable Passwords web interface. The Cisco Secure ACSes configured as this Cisco Secure ACS's replication partners are listed below this check box.

  This feature depends upon having the CiscoSecure Database Replication feature configured properly; however, replication scheduling does not apply to propagation of changed password information. Cisco Secure ACS sends changed password information immediately, regardless of replication scheduling.

  Changed password information is replicated only to Cisco Secure ACSes that are properly configured to receive replication data from this Cisco Secure ACS. The automatically triggered cascade setting for the CiscoSecure Database Replication feature does not cause Cisco Secure ACSes that receive changed password information to send it to their replication partners.

  For more information about CiscoSecure Database Replication, see CiscoSecure Database Replication, page 9-1.

- **Password Change Log File Management**—These settings enable you to configure how Cisco Secure ACS handles log files generated for the User Password Change report. For more information about this report, see Cisco Secure ACS System Logs, page 11-13.

  The log file management options for the User Password Changes Log are listed below:

  - **Generate New File**—You can specify the frequency at which Cisco Secure ACS creates a User Password Changes Log file: daily, weekly, monthly, or after the log reaches a size in kilobytes that you specify.
  - **Manage Directory**—You can specify whether Cisco Secure ACS controls the retention of log files. If enabled, this feature enables you to specify either the maximum number of files to retain or the maximum age of files to retain. If the maximum number of files is exceeded, Cisco Secure ACS deletes the oldest log file. If the maximum age of a file is exceeded, Cisco Secure ACS deletes the file.



Downloaded from www.Manualslib.com manuals search engine

# Configuring Local Password Management

To configure password validation options, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Local Password Management**.

The Local Password Management page appears.

**Step 3** Under Password Validation Options, follow these steps:

**a.** In Password length between *X* and *Y* characters, type the *minimum* valid number of characters for a password in the *X* box. While the *X* box accepts two characters, passwords can only be between 1 and 32 characters in length.

**b.** In Password length between *X* and *Y* characters, type the *maximum* valid number of characters for a password in the *Y* box. While the *X* box accepts two characters, passwords can only be between 1 and 32 characters in length.

**c.** If you want to disallow passwords that contain the username, select the **Password may not contain the username** check box.

**d.** If you want to require that a user password must be different than the previous user password, select the **Password is different from the previous value** check box.

**e.** If you want to require that passwords must contain both letters and numbers, select the **Password must be alphanumeric** check box.

**Step 4** Under Remote Change Password, follow these steps:

**a.** If you want to *enable* user password changes in Telnet sessions, clear the **Disable TELNET Change Password against this ACS and return the following message to the users telnet session** check box.

**b.** If you want to *disable* user password changes in Telnet sessions, select the **Disable TELNET Change Password against this ACS and return the following message to the users telnet session** check box.

**c.** In the box below the **Disable TELNET Change Password against this ACS and return the following message to the users telnet session** check box, type a message that users should see when attempting to change a password in a Telnet session and when the Telnet password change feature has been disabled (Step b).



Downloaded from www.Manualslib.com manuals search engine

d. If you want Cisco Secure ACS to send changed password information immediately after a user has changed a password, select the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.

**Tip** The Cisco Secure ACSes that receive the changed password information list below the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.

**Step 5** If you want Cisco Secure ACS to generate a new User Password Changes log file at a regular interval, select one of the following options:

- **Every day**—Cisco Secure ACS generates a new User Password Changes log file at the start of each day.
- **Every week**—Cisco Secure ACS generates a new User Password Changes log file at the start of each week.
- **Every month**—Cisco Secure ACS generates a new User Password Changes log file at the start of each month.

**Step 6** If you want Cisco Secure ACS to generate a new User Password Changes log file when the current file reaches a specific size, select the **When size is greater than** *X* **KB** option and type the file size threshold, in kilobytes, in the *X* box.

**Step 7** If you want to manage which User Password Changes log files Cisco Secure ACS keeps, follow these steps:

a. Select the **Manage Directory** check box.

b. If you want to limit the number of User Password Changes log files Cisco Secure ACS retains, select the **Keep only the last** *X* **files** option and type the number of files you want Cisco Secure ACS to retain in the *X* box.

c. If you want to limit how old User Password Changes log files retained by Cisco Secure ACS can be, select the **Delete files older than** *X* **days** option and type the number of days for which Cisco Secure ACS should retain a User Password Changes log file before deleting it.

**Step 8** Click **Submit**.

Cisco Secure ACS restarts its services and implements the settings you specified.



Downloaded from www.Manualslib.com manuals search engine

# Cisco Secure ACS Backup

This section provides information about the Cisco Secure ACS Backup feature, including procedures for implementing this feature.

This section contains the following topics:


- About Cisco Secure ACS Backup, page 8-9
- Backup File Locations, page 8-10
- Directory Management, page 8-10
- Components Backed Up, page 8-10
- Reports of Cisco Secure ACS Backups, page 8-11
- Backup Options, page 8-11
- Performing a Manual Cisco Secure ACS Backup, page 8-12
- Scheduling Cisco Secure ACS Backups, page 8-12
- Disabling Scheduled Cisco Secure ACS Backups, page 8-13


## About Cisco Secure ACS Backup

The ACS Backup feature backs up your Cisco Secure ACS system information to a file on the local hard drive. You can manually back up the Cisco Secure ACS system. You can also establish automated backups that occur at regular intervals or at selected days of the week and times. Maintaining backup files can minimize downtime if system information becomes corrupt or is misconfigured. We recommend copying the files to the hard drive on another system in case the hardware fails on the primary system.

For information about using a backup file to restore Cisco Secure ACS, see Cisco Secure ACS System Restore, page 8-14.

## Backup File Locations

The default directory for backup files is the following:

*drive*:*path*\CSAuth\System Backups



Downloaded from www.Manualslib.com manuals search engine

where *drive* is the local drive where you installed Cisco Secure ACS and *path* is the path from the root of *drive* to the Cisco Secure ACS directory. For example, if you installed Cisco Secure ACS version 3.0 in the default location, the default backup location would be

```
c:\Program Files\CiscoSecure ACS v3.0\CSAuth\System Backups
```

The filename given to a backup is determined by Cisco Secure ACS. For more information about filenames assigned to backup files generated by Cisco Secure ACS, see Backup Filenames and Locations, page 8-15.

# Directory Management

You can configure the number of backup files to keep and the number of days after which backup files are deleted. The more complex your configuration and the more often you back up the system, the more diligent we recommend you be about clearing out old databases from the Cisco Secure ACS hard drive.

# Components Backed Up

The ACS System Backup feature backs up the Cisco Secure ACS user database and information from the Windows Registry that is relevant to Cisco Secure ACS. The user database backup includes all user information, such as username, password, and other authentication information, including server certificates and the certificate trust list. The Windows Registry information includes any system information that is stored in the Windows Registry, such as NDG information, AAA client configuration, and administrator accounts.

# Reports of Cisco Secure ACS Backups

When a system backup takes place, whether it was manually generated or scheduled, the event is logged in the Administration Audit report and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of Cisco Secure ACS.

For more information about Cisco Secure ACS reports, see Chapter 1, “Overview”.



Downloaded from www.Manualslib.com manuals search engine

# Backup Options

The ACS System Backup Setup page contains the following configuration options:

- **Manually**—Cisco Secure ACS does not perform automatic backups. When this option is selected, you can only perform a backup by following the steps in Performing a Manual Cisco Secure ACS Backup, page 8-12.
- **Every** *X* **minutes**—Cisco Secure ACS performs automatic backups on a set frequency. The unit of measurement is minutes, with a default backup frequency of 60 minutes.
- **At specific times...**—Cisco Secure ACS performs automatic backups at the time specified in the day and hour graph. The minimum interval is one hour, and the backup takes place on the hour selected.
- **Directory**—The directory where Cisco Secure ACS writes the backup file. The directory must be specified by its full path on the Windows server that runs Cisco Secure ACS, such as `c:\acs-bups`.
- **Manage Directory**—Defines whether Cisco Secure ACS deletes older backup files. Using the following options, you can specify how Cisco Secure ACS determines which log files to delete:
  - **Keep only the last** *X* **files**—Cisco Secure ACS retains the most recent backup files, up to the number of files specified. When the number of files specified is exceeded, Cisco Secure ACS deletes the oldest files.
  - **Delete files older than** *X* **days**—Cisco Secure ACS deletes backup files that are older than the number of days specified. When a backup file grows older than the number of days specified, Cisco Secure ACS deletes it.

# Performing a Manual Cisco Secure ACS Backup

You can back up Cisco Secure ACS whenever you want, without scheduling the backup.

To perform an immediate backup of Cisco Secure ACS, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Click **ACS Backup**.

The ACS System Backup Setup page appears.

**Step 3** In the Directory box under Backup Location, type the drive and path to the directory on a local hard drive where you want the backup file to be written.

**Step 4** Click **Backup Now**.

Cisco Secure ACS immediately begins a backup.

# Scheduling Cisco Secure ACS Backups

You can schedule Cisco Secure ACS backups to occur at regular intervals or on selected days of the week and times.

To schedule the times at which Cisco Secure ACS performs a backup, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Backup**.

The ACS System Backup Setup page appears.

**Step 3** To schedule backups at regular intervals, under ACS Backup Scheduling, select the **Every** *X* **minutes** option and in the *X* box type the length of the interval at which Cisco Secure ACS should perform backups.

**Note** Because Cisco Secure ACS is momentarily shut down during backup, if the backup interval is too frequent, users might be unable to authenticate.

**Step 4** To schedule backups at specific times, follow these steps:

**a.** Under ACS Backup Scheduling, select the **At specific times** option.

**b.** In the day and hour graph, click the times at which you want Cisco Secure ACS to perform a backup.



Downloaded from www.Manualslib.com manuals search engine

**Tip** Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

**Step 5** To change the location where Cisco Secure ACS writes backup files, type the drive letter and path in the Directory box.

**Step 6** To manage which backup files Cisco Secure ACS keeps, follow these steps:

a. Select the **Manage Directory** check box.

b. To limit the number of backup files Cisco Secure ACS retains, select the **Keep only the last** *X* **files** option and type in the *X* box the number of files you want Cisco Secure ACS to retain.

c. To limit how old backup files retained by Cisco Secure ACS can be, select the **Delete files older than** *X* **days** option and type the number of days for which Cisco Secure ACS should retain a backup file before deleting it.

**Step 7** Click **Submit**.

Cisco Secure ACS implements the backup schedule you configured.

# Disabling Scheduled Cisco Secure ACS Backups

You can disable scheduled Cisco Secure ACS backups without losing the schedule itself. This allows you to end scheduled backups and resume them later without having to re-create the schedule.

To disable a scheduled backup, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Backup**.

The ACS System Backup Setup page appears.

**Step 3** Under ACS Backup Scheduling, select the **Manual** option.

**Step 4** Click **Submit**.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS does not continue any scheduled backups. You can still perform manual backups as needed.

# Cisco Secure ACS System Restore

This section provides information about the Cisco Secure ACS System Restore feature, including procedures for restoring your Cisco Secure ACS from a backup file.

This section contains the following topics:


- About Cisco Secure ACS System Restore, page 8-14
- Backup Filenames and Locations, page 8-15
- Components Restored, page 8-16
- Reports of Cisco Secure ACS Restorations, page 8-16
- Restoring Cisco Secure ACS from a Backup File, page 8-16


## About Cisco Secure ACS System Restore

The ACS System Restore feature enables you to restore your system configuration from backup files generated by the ACS Backup feature. This feature helps minimize downtime if Cisco Secure ACS system information becomes corrupted or is misconfigured.

The ACS System Restore feature only works with backup files generated by a Cisco Secure ACS running an identical Cisco Secure ACS version and patch level.

## Backup Filenames and Locations

The ACS System Restore feature restores the Cisco Secure ACS user database and Cisco Secure ACS Windows Registry information from a file that was created by the ACS Backup feature. Cisco Secure ACS writes backup files only on the local



Downloaded from www.Manualslib.com manuals search engine

hard drive. You can restore from any backup file you select. For example, you can restore from the latest backup file, or if you suspect that the latest backup was incorrect, you can select an earlier backup file to restore from.

The backup directory is selected when you schedule backups or perform a manual backup. The default directory for backup files is the following:

*drive*:*path*\CSAuth\System Backups

where *drive* is the local drive where you installed Cisco Secure ACS and *path* is the path from the root of *drive* to the Cisco Secure ACS directory. For example, if you installed Cisco Secure ACS version 3.0 in the default location, the default backup location would be:

```
c:\Program Files\CiscoSecure ACS v3.0\CSAuth\System Backups
```

Cisco Secure ACS creates backup files using the date and time format:

*dd-mmm-yyyy hh-nn-ss*.dmp

where:

- *dd* is the date the backup started
- *mmm* is the month, abbreviated in alphabetic characters
- *yyyy* is the year
- *hh* is the hour, in 24-hour format
- *nn* is the minute
- *ss* is the second at which the backup started

For example, if Cisco Secure ACS started a backup on October 13, 1999, 11:41:35 a.m., Cisco Secure ACS would generate a backup file named:

```
13-Oct-1999 11-41-35.dmp
```

If you are not sure of the location of the latest backup file, check your scheduled backup configuration on the ACS Backup page.

# Components Restored

You can select the components to restore: the user and group databases, the system configuration, or both.



Downloaded from www.Manualslib.com manuals search engine

# Reports of Cisco Secure ACS Restorations

When a Cisco Secure ACS system restoration takes place, the event is logged in the Administration Audit report and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of Cisco Secure ACS.

For more information about Cisco Secure ACS reports, see Chapter 1, "Overview".

# Restoring Cisco Secure ACS from a Backup File

You can perform a system restoration of Cisco Secure ACS whenever needed.

**Note** Using the Cisco Secure ACS System Restore feature restarts all Cisco Secure ACS services and logs out all administrators.

To restore Cisco Secure ACS from a backup file generated by the Cisco Secure ACS Backup feature, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Restore**.

The ACS System Restore Setup page appears.

The Directory box displays the drive and path to the backup directory most recently configured in the Directory box on the ACS Backup page.

Beneath the Directory box, Cisco Secure ACS displays the backup files in the current backup directory. If no backup files exist, `<No Matching Files>` appears in place of filenames.

**Step 3** To change the backup directory, type the new drive and path to the backup directory in the Directory box, and then click **OK**.

Cisco Secure ACS displays the backup files, if any, in the backup directory you specified.

**Step 4** In the list below the Directory box, select the backup file you want to use to restore Cisco Secure ACS.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** To restore user and group database information, select the **User and Group Database** check box.

**Step 6** To restore system configuration information, select the **CiscoSecure ACS System Configuration** check box.

**Step 7** Click **Restore Now**.

Cisco Secure ACS displays a confirmation dialog box indicating that performing the restoration will restart Cisco Secure ACS services and log out all administrators.

**Step 8** To continue with the restoration, click **OK**.

Cisco Secure ACS restores the system components specified using the backup file you selected. The restoration should require several minutes to complete, depending on which components you selected to restore and the size of your database.

When the restoration is complete, you can log in again to Cisco Secure ACS.

# Cisco Secure ACS Active Service Management

ACS Active Service Management is an application-specific service monitoring tool that is tightly integrated with ACS. The two features that compose ACS Active Service Management are described in this section.

This section contains the following topics:


- System Monitoring, page 8-18
- Event Logging, page 8-20


## System Monitoring

Cisco Secure ACS system monitoring enables you to determine how often Cisco Secure ACS tests its authentication and accounting processes, and to determine what automated actions it takes should tests detect a failure of these processes. Cisco Secure ACS accomplishes system monitoring with the CSMon service. For more information about the CSMon service, see CSMon, page G-4.



Downloaded from www.Manualslib.com manuals search engine

## System Monitoring Options

You have the following options for configuring system monitoring:

- **Test login process every *X* minutes**—Controls whether or not Cisco Secure ACS tests its login process. The value in the X box defines, in minutes, how often Cisco Secure ACS tests its login process. The default frequency is once per minute, which is also the most frequent testing interval possible.

  When this option is enabled, at the interval defined, Cisco Secure ACS tests authentication and accounting. If the test fails, after four unsuccessful re-tries Cisco Secure ACS performs the action identified in the If no successful authentications are recorded list and logs the event.

- **If no successful authentications are recorded**—Specifies what action Cisco Secure ACS takes if it detects that its test login process failed. This list contains several built-in actions and reflects actions that you define. The items beginning with asterisks (*) are predefined actions.
  - ***Restart All**—Restart all Cisco Secure ACS services.
  - ***Restart RADIUS/TACACS+**—Restart only the RADIUS and TACACS+ services.
  - ***Reboot**—Reboot Cisco Secure ACS.
  - **Custom actions**—You can define other actions for Cisco Secure ACS to take upon failure of the login process. Cisco Secure ACS can execute a batch file or executable upon the failure of the login process. To make a batch or executable file available in the on failure list, place the file in the following directory:

    *drive*:*path*\CSMon\Scripts

    where *drive* is the local drive where you installed Cisco Secure ACS and *path* is the path from the root of *drive* to the Cisco Secure ACS directory.
  - **Take No Action**—Leave Cisco Secure ACS operating as is.
- **Generate event when an attempt is made to log in to a disabled account**—Specifies whether Cisco Secure ACS generates a log entry when a user attempts to log in to your network using a disabled account.
- **Log all events to the NT Event log**—Specifies whether Cisco Secure ACS generates a Windows event log entry for each exception event.



Downloaded from www.Manualslib.com manuals search engine

- **Email notification of event**—Specifies whether Cisco Secure ACS sends an e-mail notification for each event.
  - **To**—The e-mail address that notification e-mail is sent to. For example, joeadmin@company.com.
  - **SMTP Mail Server**—The simple mail transfer protocol (SMTP) server that Cisco Secure ACS should use to send notification e-mail. You can identify the SMTP server either by its hostname or by its IP address.

## Setting Up System Monitoring

To setup Cisco Secure ACS System Monitoring, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Service Management**.

The ACS Active Service Management Setup page appears.

**Step 3** To have Cisco Secure ACS test the login process, follow these steps:

**a.** Select the **Test login process every** *X* **minutes** check box.

**b.** Type in the *X* box the number of minutes (up to 3 characters) that should pass between each login process test.

**c.** From the **If no successful authentications are recorded** list, select the action Cisco Secure ACS should take when the login test fails five successive times.

**Step 4** To have Cisco Secure ACS generate a Windows event when a user attempts to log in to your network using a disabled account, select the **Generate event when an attempt is made to log in to a disabled account** check box.

**Step 5** If you want to set up event logging, see Setting Up Event Logging, page 8-20.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** If you are done setting up Cisco Secure ACS Service Management, click **Submit**.

Cisco Secure ACS implements the service management settings you made.

# Event Logging

The Event Logging feature enables you to configure whether Cisco Secure ACS logs events to the Windows event log and whether Cisco Secure ACS generates an e-mail when an event occurs. Cisco Secure ACS uses the System Monitoring feature to detect the events to be logged. For more information about system monitoring, see System Monitoring Options, page 8-18.

## Setting Up Event Logging

To view the Windows event log, select **Start > Programs > Administrative Tools > Event Viewer**. For more information about the Windows event log or Event Viewer, refer to your Microsoft Windows documentation.

To set up Cisco Secure ACS event logging, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Service Management**.

The ACS Active Service Management Setup page appears.

**Step 3** To have Cisco Secure ACS send all events to the Windows event log, select **Log all events to the Windows Event log**.

**Step 4** To have Cisco Secure ACS send an e-mail when an event occurs, follow these steps:

**a.** Select the **Email notification of event** check box.

**b.** In the To box, type the e-mail address (up to 200 characters) to which Cisco Secure ACS should send event notification e-mail.

**Note** Do not use underscores in the e-mail addresses you type in this box.



Downloaded from www.Manualslib.com manuals search engine

c. In the SMTP Mail Server box, type the hostname (up to 200 characters) of the sending e-mail server.

**Note** The SMTP mail server must be operational and must be available from the Cisco Secure ACS.

**Step 5** If you want to set up system monitoring, see Setting Up System Monitoring, page 8-19.

**Step 6** If you are done setting up Cisco Secure ACS Service Management, click **Submit**.

Cisco Secure ACS implements the service management settings you made.

# VoIP Accounting Configuration

The VoIP Accounting Configuration feature enables you to specify which accounting logs receive VoIP accounting data. There are three options for VoIP accounting:

- **Send to both RADIUS and VoIP Accounting Log Targets**—Cisco Secure ACS appends VoIP accounting data to the RADIUS accounting data and logs it separately to a CSV file. To view the data, you can use either RADIUS Accounting or VoIP Accounting under Reports and Activity.
- **Send only to VoIP Accounting Log Targets**—Cisco Secure ACS only logs VoIP accounting data to a CSV file. To view the data, you can use VoIP Accounting under Reports and Activity.
- **Send only to RADIUS Accounting Log Targets**—Cisco Secure ACS only appends VoIP accounting data to the RADIUS accounting data. To view the data, you can use RADIUS Accounting under Reports and Activity.

## Configuring VoIP Accounting

**Note** The VoIP Accounting Configuration feature does not enable VoIP accounting. To enable VoIP accounting, see Chapter 1, “Overview”.



Downloaded from www.Manualslib.com manuals search engine

To configure VoIP accounting, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **VoIP Accounting Configuration**.

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Voice-over-IP (VoIP) Accounting Configuration** check box.

The VoIP Accounting Configuration page appears. The Voice-over-IP (VoIP) Accounting Configuration table displays the options for VoIP accounting.

**Step 3** Select the VoIP accounting option you want.

**Step 4** Click **Submit**.

Cisco Secure ACS implements the VoIP accounting configuration you specified.



Downloaded from www.Manualslib.com manuals search engine

# System Configuration: Advanced

This chapter addresses the CiscoSecure Database Replication and RDBMS Synchronization features found in the System Configuration section of Cisco Secure ACS for Windows Server. It contains the following sections:

This chapter contains the following topics:


- CiscoSecure Database Replication, page 9-1
- RDBMS Synchronization, page 9-25
- IP Pools Server, page 9-44
- IP Pools Address Recovery, page 9-51


## CiscoSecure Database Replication

This section provides information about the CiscoSecure Database Replication feature, including procedures for implementing this feature and configuring the Cisco Secure ACSes involved.

This section contains the following topics:


- About CiscoSecure Database Replication, page 9-2
  - Replication Process, page 9-4
  - Replication Frequency, page 9-7
- Important Implementation Considerations, page 9-7
- Database Replication Versus Database Backup, page 9-10
- Database Replication Logging, page 9-10




Downloaded from www.Manualslib.com manuals search engine

- Replication Options, page 9-11
  - Replication Components Options, page 9-11
  - Outbound Replication Options, page 9-12
  - Inbound Replication Options, page 9-15
- Implementing Primary and Secondary Replication Setups on Cisco Secure ACSes, page 9-15
- Configuring a Secondary Cisco Secure ACS, page 9-17
- Replicating Immediately, page 9-19
- Scheduling Replication, page 9-21
- Disabling CiscoSecure Database Replication, page 9-24
- Database Replication Event Errors, page 9-25


# About CiscoSecure Database Replication

Database replication creates mirror systems of Cisco Secure ACSes by duplicating parts of the primary Cisco Secure ACS setup to one or more secondary Cisco Secure ACSes. You can configure your AAA clients to use these secondary Cisco Secure ACSes if the primary Cisco Secure ACS fails or is unreachable. With a secondary Cisco Secure ACS whose CiscoSecure database is a replica of the CiscoSecure database on the primary Cisco Secure ACS, if the primary Cisco Secure ACS goes out of service, incoming requests are authenticated without network downtime, provided that your AAA clients are configured to failover to the secondary Cisco Secure ACS.

Database replication allows you to do the following:

- Select the parts of the primary Cisco Secure ACS configuration to be replicated.
- Control the timing of the replication process, including creating schedules.
- Export selected configuration items from the primary Cisco Secure ACS.
- Securely transport selected configuration data from the primary Cisco Secure ACS to one or more secondary Cisco Secure ACSes.
- Update the secondary Cisco Secure ACSes to create matching configurations.

The following items cannot be replicated:



Downloaded from www.Manualslib.com manuals search engine

- IP pool definitions (for more information, see About IP Pools Server, page 9-44).
- Cisco Secure ACS certificate and private key files.
- All external user database configurations, including Network Admission Control (NAC) databases.
- Unknown user group mapping configuration.
- User-defined RADIUS dictionaries (for more information, see Important Implementation Considerations, page 9-7).
- Settings on the ACS Service Management page in the System Configuration section.
- All logging configurations.
- RDBMS Synchronization settings.
- Third-party software, such as Novell Requestor or RSA ACE client software.

With regard to database replication, we make the following distinctions about Cisco Secure ACSes:

- **Primary Cisco Secure ACS**—A Cisco Secure ACS that sends replicated CiscoSecure database components to other Cisco Secure ACSes.
- **Secondary Cisco Secure ACS**—A Cisco Secure ACS that receives replicated CiscoSecure database components from a primary Cisco Secure ACS. In the HTML interface, these are identified as replication partners.

A Cisco Secure ACS can be both a primary Cisco Secure ACS and a secondary Cisco Secure ACS, provided that it is not configured to be a secondary Cisco Secure ACS to a Cisco Secure ACS for which it performs as a primary Cisco Secure ACS.

**Note** Bidirectional replication, wherein an Cisco Secure ACS both sends database components to and receives database components from the same remote Cisco Secure ACS, is not supported. Replication fails if a Cisco Secure ACS is configured to replicate to and from the same Cisco Secure ACS.

**Note** All Cisco Secure ACSes involved in replication must run the same release of the Cisco Secure ACS software. For example, if the primary Cisco Secure ACS is running Cisco Secure ACS version 3.2, all secondary Cisco Secure ACSes should



Downloaded from www.Manualslib.com manuals search engine

be running Cisco Secure ACS version 3.2. Because patch releases can introduce significant changes to the CiscoSecure database, we strongly recommend that Cisco Secure ACSes involved in replication use the same patch level, too.

## Replication Process

This topic describes the process of database replication, including the interaction between a primary Cisco Secure ACS and each of its secondary Cisco Secure ACSes. The following steps occur in database replication:

1. The primary Cisco Secure ACS determines if its database has changed since the last successful replication. If it has, replication proceeds. If it has not, replication is aborted. No attempt is made to compare the databases of the primary and secondary Cisco Secure ACSes.

**Tip** You can force replication to occur by making one change to a user or group profile, such as changing a password or modifying a RADIUS attribute.

2. The primary Cisco Secure ACS contacts the secondary Cisco Secure ACS. In this initial connection, the following four events occur:
   a. The two Cisco Secure ACSes perform mutual authentication based upon the shared secret of the primary Cisco Secure ACS. If authentication fails, replication fails.

**Note** On the secondary Cisco Secure ACS, the AAA Servers table entry for the primary Cisco Secure ACS must have the same shared secret that the primary Cisco Secure ACS has for itself in its own AAA Servers table entry. The secondary Cisco Secure ACS's shared secret is irrelevant.

   b. The secondary Cisco Secure ACS verifies that it is not configured to replicate to the primary Cisco Secure ACS. If it is, replication is aborted. Cisco Secure ACS does not support bidirectional replication, wherein a Cisco Secure ACS can act as both a primary and a secondary Cisco Secure ACS to the same remote Cisco Secure ACS.



Downloaded from www.Manualslib.com manuals search engine

c. The primary Cisco Secure ACS verifies that the version of Cisco Secure ACS that the secondary Cisco Secure ACS is running is the same as its own version of Cisco Secure ACS. If not, replication fails.

d. The primary Cisco Secure ACS compares the list of database components it is configured to send with the list of database components the secondary Cisco Secure ACS is configured to receive. If the secondary Cisco Secure ACS is not configured to receive any of the components that the primary Cisco Secure ACS is configured to send, the database replication fails.

3. After the primary Cisco Secure ACS has determined which components to send to the secondary Cisco Secure ACS, the replication process continues on the primary Cisco Secure ACS as follows:

   a. The primary Cisco Secure ACS stops its authentication and creates a copy of the CiscoSecure database components that it is configured to replicate. During this step, if AAA clients are configured properly, those that usually use the primary Cisco Secure ACS failover to another Cisco Secure ACS.

   b. The primary Cisco Secure ACS resumes its authentication service. It also compresses and encrypts the copy of its database components for transmission to the secondary Cisco Secure ACS.

   c. The primary Cisco Secure ACS transmits the compressed, encrypted copy of its database components to the secondary Cisco Secure ACS. This transmission occurs over a TCP connection, using port 2000. The TCP session uses a 128-bit encrypted, Cisco-proprietary protocol.

4. After the preceding events on the primary Cisco Secure ACS, the database replication process continues on the secondary Cisco Secure ACS as follows:

   a. The secondary Cisco Secure ACS receives the compressed, encrypted copy of the CiscoSecure database components from the primary Cisco Secure ACS. After transmission of the database components is complete, the secondary Cisco Secure ACS decompresses the database components.

   b. The secondary Cisco Secure ACS stops its authentication service and replaces its database components with the database components it received from the primary Cisco Secure ACS. During this step, if AAA clients are configured properly, those that usually use the secondary Cisco Secure ACS failover to another Cisco Secure ACS.



Downloaded from www.Manualslib.com manuals search engine

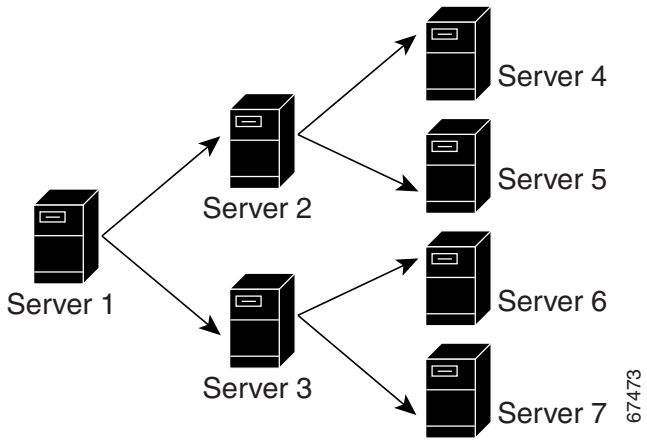
c. The secondary Cisco Secure ACS resumes its authentication service.

Cisco Secure ACS can act as both a primary Cisco Secure ACS and a secondary Cisco Secure ACS. Figure 9-1 shows a cascading replication scenario. Server 1 acts only as a primary Cisco Secure ACS, replicating to servers 2 and 3, which act as secondary Cisco Secure ACSes. After replication from server 1 to server 2 has completed, server 2 acts as a primary Cisco Secure ACS while replicating to servers 4 and 5. Similarly, server 3 acts as a primary Cisco Secure ACS while replicating to servers 6 and 7.

**Note** If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary Cisco Secure ACS with all Cisco Secure ACSes that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary Cisco Secure ACS. In Figure 9-1, server 1 must have an entry in its AAA Servers table for each of the other six Cisco Secure ACSes. If this is not done, after replication, servers 2 and 3 do not have servers 4 through 7 in their AAA Servers tables and replication will fail.

If server 2 were configured to replicate to server 1 in addition to receiving replication from server 1, replication to server 2 would fail. Cisco Secure ACS cannot support such a configuration, known as bidirectional replication. To safeguard against this, a secondary Cisco Secure ACS aborts replication when its primary Cisco Secure ACS appears on its Replication list.

***Figure 9-1 Cascading Database Replication***






Downloaded from www.Manualslib.com manuals search engine

## Replication Frequency

The frequency with which your Cisco Secure ACSes replicate can have important implications for overall AAA performance. With shorter replication frequencies, a secondary Cisco Secure ACS is more up-to-date with the primary Cisco Secure ACS. This allows for a more current secondary Cisco Secure ACS if the primary Cisco Secure ACS fails.

There is a cost to having frequent replications. The more frequent the replication, the higher the load on a multi-Cisco Secure ACS architecture and on your network environment. If you schedule frequent replication, network traffic is much higher. Also, processing load on the replicating systems is increased. Replication consumes system resources and briefly interrupts authentication; thus the more often replication is repeated, the greater the impact on the AAA performance of the Cisco Secure ACS.

**Note** Regardless of how frequently replication is scheduled to occur, it only occurs when the database of the primary Cisco Secure ACS has changed since the last successful replication.

This issue is more apparent with databases that are large or that frequently change. Database replication is a non-incremental, destructive backup. In other words, it completely replaces the database and configuration on the secondary Cisco Secure ACS every time it runs. Therefore, a large database results in substantial amounts of data being transferred, and the processing overhead can also be large.

# Important Implementation Considerations

You should consider several important points when you implement the CiscoSecure Database Replication feature:

- Cisco Secure ACS only supports database replication to other Cisco Secure ACSes. All Cisco Secure ACSes participating in CiscoSecure database replication must run the same version of Cisco Secure ACS. We strongly recommend that Cisco Secure ACSes involved in replication use the same patch level, too.
- You must ensure correct configuration of the AAA Servers table in all Cisco Secure ACSes involved in replication.



Downloaded from www.Manualslib.com manuals search engine

- In its AAA Servers table, a primary Cisco Secure ACS must have an accurately configured entry for each secondary Cisco Secure ACS.

**Note** If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary Cisco Secure ACS with all Cisco Secure ACSes that will receive replicated database components, regardless of whether they receive replication directly or indirectly from that primary Cisco Secure ACS. For example, if the primary Cisco Secure ACS replicates to two secondary Cisco Secure ACSes which, in turn, each replicate to two more Cisco Secure ACSes, the primary Cisco Secure ACS must have AAA server configurations for all six Cisco Secure ACSes that will receive replicated database components.

- In its AAA Servers table, a secondary Cisco Secure ACS must have an accurately configured entry for each of its primary Cisco Secure ACSes.
- On a primary Cisco Secure ACS and all its secondary Cisco Secure ACSes, the AAA Servers table entries for the primary Cisco Secure ACS must have identical shared secrets.

- Only suitably configured, valid Cisco Secure ACSes can be secondary Cisco Secure ACSes. To configure a secondary Cisco Secure ACS for database replication, see Configuring a Secondary Cisco Secure ACS, page 9-17.
- Replication only occurs when the database of the primary Cisco Secure ACS has changed since the last successful replication, regardless of how frequently replication is scheduled to occur. When a scheduled or manually started replication begins, the primary Cisco Secure ACS automatically aborts replication if its database has not changed since the last successful replication.

**Tip** You can force replication to occur by making one change to a user or group profile, such as changing a password or modifying a RADIUS attribute.

- Replication to secondary Cisco Secure ACSes takes place sequentially in the order listed in the Replication list under Replication Partners on the CiscoSecure Database Replication page.



Downloaded from www.Manualslib.com manuals search engine

- A secondary Cisco Secure ACS receiving replicated components must be configured to accept database replication from the primary Cisco Secure ACS. To configure a secondary Cisco Secure ACS for database replication, see Configuring a Secondary Cisco Secure ACS, page 9-17.
- Cisco Secure ACS does not support bidirectional database replication. The secondary Cisco Secure ACS receiving the replicated components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated components. If so, it rejects the components.
- If you replicate user accounts, be sure to name external database configurations identically on primary and secondary Cisco Secure ACSes. A replicated user account retains its association with the database assigned to provide authentication or posture validation service, regardless of whether a database configuration of the same name exists on the secondary Cisco Secure ACS. For example, if user account is associated with a database named “WestCoast LDAP” on the primary Cisco Secure ACS, the replicated user account on all secondary Cisco Secure ACSes remains associated with an external user database named “WestCoast LDAP” even if you have not configured an LDAP database instance of that name.
- If you replicate NAC policies, secondary Cisco Secure ACSes associate policies to NAC databases by the order in which the NAC databases were created, not by the database name. For example, if the primary Cisco Secure ACS has the following NAC database and policy configuration:
  - “NAC DB One” with “Policy One” selected.
  - “NAC DB Two” with “Policy Two” selected.

  and if a secondary Cisco Secure ACS is configured first with a NAC database named “NAC DB Two” and second with a NAC database named “NAC DB One”, then the following policy selection results after replication occurs:
  - “NAC DB One” with “Policy Two” selected.
  - “NAC DB Two” with “Policy One” selected.
- To replicate user and group settings that use user-defined RADIUS vendor and VSAs, you must manually add the user-defined RADIUS vendor and VSA definitions on primary and secondary Cisco Secure ACSes, making sure that the RADIUS vendor slots that the user-defined RADIUS vendors occupy are identical on each Cisco Secure ACS. After you have done so, replication



Downloaded from www.Manualslib.com manuals search engine

of settings using user-defined RADIUS vendors and VSAs is supported. For more information about user-defined RADIUS vendors and VSAs, see Custom RADIUS Vendors and VSAs, page 9-28.

# Database Replication Versus Database Backup

Do not confuse database replication with system backup. Database replication does *not* replace System Backup. While both features protect against partial or complete server loss, each feature addresses the issue in a different way.

System Backup archives data into a format that you can later use to restore the configuration if the system fails or the data becomes corrupted. The backup data is stored on the local hard drive and can be copied and removed from the system for long-term storage. You can store several generations of database backup files.

CiscoSecure Database Replication enables you to copy various components of the CiscoSecure database to other Cisco Secure ACSes. This can help you plan a failover AAA architecture and can reduce the complexity of your configuration and maintenance tasks. While it is unlikely, it is possible that CiscoSecure Database Replication can propagate a corrupted database to the Cisco Secure ACSes that generate your backup files.

**Caution** Because the possibility of replicating a corrupted database always exists, we strongly recommend that you implement a backup plan, especially in mission-critical environments. For more information about backing up Cisco Secure ACS or the CiscoSecure database, see Cisco Secure ACS Backup, page 8-9 and Appendix D, "CSUtil Database Utility".

# Database Replication Logging

Cisco Secure ACS logs all replication events—whether successful or not—in two files:

- The Windows Event Log
- The Database Replication report

To view the Windows Event Log, use the Windows administration utilities. You can view recent reports in the Reports and Activity section of Cisco Secure ACS.



Downloaded from www.Manualslib.com manuals search engine

For more information about Cisco Secure ACS reports, see Chapter 1, "Overview".

# Replication Options

The Cisco Secure ACS HTML interface provides three sets of options for configuring CiscoSecure Database Replication, documented in this section.

This section contains the following topics:


- Replication Components Options, page 9-11
- Outbound Replication Options, page 9-12
- Inbound Replication Options, page 9-15


## Replication Components Options

You can specify both the CiscoSecure database components that a Cisco Secure ACS sends as a primary Cisco Secure ACS and the components that it receives as a secondary Cisco Secure ACS.

**Note** The CiscoSecure database components received by a secondary Cisco Secure ACS *overwrite* the CiscoSecure database components on the secondary Cisco Secure ACS. Any information unique to the overwritten database component is lost.

The Replication Components table on the CiscoSecure Database Replication page presents the options that control which components are replicated; these options are as follows:

- **User and group database**—Replicate information for groups and users. Using this option excludes the use of the "Group database only" option.
- **Group database only**—Replicate information for groups, but not for users. Using this option excludes the use of the "User and group database" option.
- **Network Configuration Device tables**—Replicate the AAA Servers tables and the AAA Clients tables in the Network Configuration section. This also controls whether NDGs are replicated.



Downloaded from www.Manualslib.com manuals search engine

**Note** If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary Cisco Secure ACS with all Cisco Secure ACSes that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary Cisco Secure ACS. For example, if the primary Cisco Secure ACS replicates to two secondary Cisco Secure ACSes which, in turn, each replicate to two more Cisco Secure ACSes, the primary Cisco Secure ACS must have AAA server configurations for all six Cisco Secure ACSes that will receive replicated database components.

- **Distribution table**—Replicate the Proxy Distribution Table in the Network Configuration section.
- **Interface configuration**—Replicate Advanced Options settings, RADIUS settings, and TACACS+ settings from the Interface Configuration section.
- **Interface security settings**—Replicate administrators and security information for the Cisco Secure ACS HTML interface.
- **Password validation settings**—Replicate password validation settings.
- **EAP-FAST master keys and policies**—Replicate active and retired master keys and policies for EAP-FAST.
- **CNAC policies**—Replicate NAC local policies, external policies, and attribute definitions.

If mirroring the entire database might send confidential information to the secondary Cisco Secure ACS, such as the Proxy Distribution Table, you can configure the primary Cisco Secure ACS to send only a specific category of database information.

## Outbound Replication Options

In the Outbound Replication table on the CiscoSecure Database Replication page, you can schedule outbound replication and you can specify the secondary Cisco Secure ACSes for this primary Cisco Secure ACS.

- **Scheduling Options**—You can specify when CiscoSecure database replication occurs. The options that control when replication occurs appear in the Scheduling section of Outbound Replication table and are as follows:



Downloaded from www.Manualslib.com manuals search engine

- **Manually**—Cisco Secure ACS does not perform automatic database replication.
- **Automatically Triggered Cascade**—Cisco Secure ACS performs database replication to the configured list of secondary Cisco Secure ACSes when database replication from a primary Cisco Secure ACS completes. This enables you to build a propagation hierarchy of Cisco Secure ACS, relieving a primary Cisco Secure ACS from the burden of propagating the replicated components to every other Cisco Secure ACS. For an illustration of cascade replication, see Figure 9-1.

**Note** If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary Cisco Secure ACS with all Cisco Secure ACSes that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary Cisco Secure ACS. For example, if the primary Cisco Secure ACS replicates to two secondary Cisco Secure ACSes which, in turn, each replicate to two more Cisco Secure ACSes, the primary Cisco Secure ACS must have AAA server configurations for all six Cisco Secure ACSes that will receive replicated database components.

- **Every *X* minutes**—Cisco Secure ACS performs, on a set frequency, database replication to the configured list of secondary Cisco Secure ACSes. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times...**—Cisco Secure ACS performs, at the time specified in the day and hour graph, database replication to the configured list of secondary Cisco Secure ACSes. The minimum interval is one hour, and the replication takes place on the hour selected.

- **Partner Options**—You can specify the secondary Cisco Secure ACSes for this primary Cisco Secure ACS. The options that control the secondary Cisco Secure ACSes to which a primary Cisco Secure ACS replicates appear in the Partners section of the Outbound Replication table.



Downloaded from www.Manualslib.com manuals search engine

**Note** The items in the AAA Server and Replication lists reflect the AAA servers configured in the AAA Servers table in Network Configuration. To make a particular Cisco Secure ACS available as a secondary Cisco Secure ACS, you must first add that Cisco Secure ACS to the AAA Servers table of the primary Cisco Secure ACS.

  - **AAA Server**—This list represents the secondary Cisco Secure ACSes that this primary Cisco Secure ACS *does not* send replicated components to.
  - **Replication**—This list represents the secondary Cisco Secure ACSes that this primary Cisco Secure ACS *does* send replicated components to.

- **Replication timeout**—Use this text box to specify the number of minutes that this primary Cisco Secure ACS continues replicating to a secondary Cisco Secure ACS. When the timeout value is exceeded, Cisco Secure ACS terminates replication to the secondary Cisco Secure ACS is was attempting to replicate to and then it restarts the CSAuth service. The replication timeout feature helps prevent loss of AAA services due to stalled replication communication, which can occur when the network connection between the primary and secondary Cisco Secure ACS is abnormally slow or when a fault occurs within either Cisco Secure ACS. The default value is five minutes.

**Tip** The size of the components replicated affects the time required for replication. For example, replicating a user database containing 80,000 user profiles takes more time than replicating a user database containing 500 user profiles. You may need to monitor successful replication events to determine a reasonable timeout value for your implementation.

**Note** Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS receiving replicated components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated components. If so, it rejects the components.



Downloaded from www.Manualslib.com manuals search engine

## Inbound Replication Options

You can specify the primary Cisco Secure ACSes from which a secondary Cisco Secure ACS accepts replication. This option appears in the Inbound Replication table on the CiscoSecure Database Replication page.

The **Accept replication from** list controls which Cisco Secure ACSes the current Cisco Secure ACS does accept replicated components from. The list contains the following options:

- **Any Known CiscoSecure ACS Server**—If this option is selected, Cisco Secure ACS accepts replicated components from any Cisco Secure ACS configured in the AAA Servers table in Network Configuration.
- **Other AAA servers**—The list displays all the AAA servers configured in the AAA Servers table in Network Configuration. If a specific AAA server name is selected, Cisco Secure ACS accepts replicated components only from the Cisco Secure ACS specified.

**Note** Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS receiving replicated components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated components. If so, it rejects the components.

For more information about the AAA Servers table in Network Configuration, see AAA Server Configuration, page 4-21.

# Implementing Primary and Secondary Replication Setups on Cisco Secure ACSes

If you implement a replication scheme that uses cascading replication, the Cisco Secure ACS configured to replicate only when it has received replicated components from another Cisco Secure ACS acts both as a primary Cisco Secure ACS and as a secondary Cisco Secure ACS. First, it acts as a secondary Cisco Secure ACS while it receives replicated components, and then it acts as a primary Cisco Secure ACS while it replicates components to other Cisco Secure ACSes. For an illustration of cascade replication, see Figure 9-1.



Downloaded from www.Manualslib.com manuals search engine

To implement primary and secondary replication setups on Cisco Secure ACSes, follow these steps:

**Step 1** On each secondary Cisco Secure ACS, follow these steps:

**a.** In the Network Configuration section, add the primary Cisco Secure ACS to the AAA Servers table.

For more information about adding entries to the AAA Servers table, see AAA Server Configuration, page 4-21.

**b.** Configure the secondary Cisco Secure ACS to receive replicated components. For instructions, see Configuring a Secondary Cisco Secure ACS, page 9-17.

**Step 2** On the primary Cisco Secure ACS, follow these steps:

**a.** In the Network Configuration section, add each secondary Cisco Secure ACS to the AAA Servers table.

**Note** If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary Cisco Secure ACS with all Cisco Secure ACSes that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary Cisco Secure ACS. For example, if the primary Cisco Secure ACS replicates to two secondary Cisco Secure ACSes which, in turn, each replicate to two more Cisco Secure ACSes, the primary Cisco Secure ACS must have AAA server configurations for all six Cisco Secure ACSes that will receive replicated database components.

For more information about adding entries to the AAA Servers table, see AAA Server Configuration, page 4-21.

**b.** If you want to replicate according to a schedule, at intervals, or whenever the primary Cisco Secure ACS has received replicated components from another Cisco Secure ACS, see Scheduling Replication, page 9-21.

**c.** If you want to initiate replication immediately, see Replicating Immediately, page 9-19.



Downloaded from www.Manualslib.com manuals search engine

# Configuring a Secondary Cisco Secure ACS

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and select the **CiscoSecure ACS Database Replication** check box. Select the **Distributed System Settings** check box if not already selected.

The CiscoSecure Database Replication feature requires that you configure specific Cisco Secure ACSes to act as secondary Cisco Secure ACSes. The components that a secondary Cisco Secure ACS is to receive must be explicitly specified, as must be its primary Cisco Secure ACS.

Replication is always initiated by the primary Cisco Secure ACS. For more information about sending replication components, see Replicating Immediately, page 9-19 or Scheduling Replication, page 9-21.

**Caution** The CiscoSecure database components received by a secondary Cisco Secure ACS *overwrite* the CiscoSecure database components on the secondary Cisco Secure ACS. Any information unique to the overwritten database component is lost.

### Before You Begin

Ensure correct configuration of the AAA Servers table in the secondary Cisco Secure ACS. This secondary Cisco Secure ACS must have an entry in its AAA Servers table for each of its primary Cisco Secure ACSes. Also, the AAA Servers table entry for each primary Cisco Secure ACS must have the same shared secret that the primary Cisco Secure ACS has for its own entry in its AAA Servers table. For more information about the AAA Servers table, see AAA Server Configuration, page 4-21.

To configure a Cisco Secure ACS to be a secondary Cisco Secure ACS, follow these steps:

**Step 1** Log in to the HTML interface on the secondary Cisco Secure ACS.

**Step 2** In the navigation bar, click **System Configuration**.

**Step 3** Click **CiscoSecure Database Replication**.

The Database Replication Setup page appears.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** In the Replication Components table, select the **Receive** check box for each database component to be received from a primary Cisco Secure ACS.

For more information about replication components, see Replication Components Options, page 9-11.

**Step 5** Make sure that no Cisco Secure ACS that the secondary Cisco Secure ACS is to receive replicated components from is included in the Replication list. If so, select the primary Cisco Secure ACS in the Replication list and click the **<--** (left arrow) to move it to the AAA Servers list.

**Note** Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS receiving replicated components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated components. If so, it aborts replication.

**Step 6** If the secondary Cisco Secure ACS is to receive replication components from *only one* primary Cisco Secure ACS, from the Accept replication from list, select the name of the primary Cisco Secure ACS.

The primary Cisco Secure ACSes available in the Accept replication from list are determined by the AAA Servers table in the Network Configuration section. For more information about the AAA Servers table, see AAA Server Configuration, page 4-21.

**Note** On the primary Cisco Secure ACS and all secondary Cisco Secure ACSes, the AAA Servers table entries for the primary Cisco Secure ACS must have identical shared secrets.

**Step 7** If the secondary Cisco Secure ACS is to receive replication components from *more than one* primary Cisco Secure ACS, from the Accept replication from list, select **Any Known CiscoSecure ACS Server**.

The Any Known CiscoSecure ACS Server option is limited to the Cisco Secure ACSes listed in the AAA Servers table in Network Configuration.



Downloaded from www.Manualslib.com manuals search engine

**Note** For each primary Cisco Secure ACS for this secondary Cisco Secure ACS, on both the primary and secondary Cisco Secure ACS, the AAA Servers table entries for the primary Cisco Secure ACS must have identical shared secrets.

**Step 8** Click **Submit**.

Cisco Secure ACS saves the replication configuration, and at the frequency or times you specified, Cisco Secure ACS begins accepting the replicated components from the other Cisco Secure ACSes you specified.

# Replicating Immediately

You can manually start database replication.

**Note** Replication cannot occur until you have configured at least one secondary Cisco Secure ACS. For more information about configuring a secondary Cisco Secure ACS, see Configuring a Secondary Cisco Secure ACS, page 9-17.

### Before You Begin

Ensure correct configuration of the primary and secondary Cisco Secure ACSes. For detailed steps, see Implementing Primary and Secondary Replication Setups on Cisco Secure ACSes, page 9-15.

For each secondary Cisco Secure ACS that this Cisco Secure ACS is to send replicated components to, make sure that you have completed the steps in Configuring a Secondary Cisco Secure ACS, page 9-17.

To initiate database replication immediately, follow these steps:

**Step 1** Log in to the HTML interface on the primary Cisco Secure ACS.

**Step 2** In the navigation bar, click **System Configuration**.

**Step 3** Click **CiscoSecure Database Replication**.



Downloaded from www.Manualslib.com manuals search engine

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and select the **CiscoSecure ACS Database Replication** check box. Select the **Distributed System Settings** check box if not already selected.

The Database Replication Setup page appears.

**Step 4** For each CiscoSecure database component you want to replicate to a secondary Cisco Secure ACS, under Replication Components, select the corresponding **Send** check box.

**Step 5** For each secondary Cisco Secure ACS that you want the primary Cisco Secure ACS to replicate its select components to, select the secondary Cisco Secure ACS from the AAA Servers list, and then click **-->** (right arrow button).

**Tip** If you want to remove a secondary Cisco Secure ACSes from the Replication list, select the secondary Cisco Secure ACS in the Replication list, and then click **<--** (left arrow button).

**Note** Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS receiving replicated components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated components. If so, it rejects the components.

**Step 6** In the **Replication timeout** text box, specify how long this Cisco Secure ACS will perform replication to each of its secondary Cisco Secure ACS before terminating the replication attempt and restarting the CSAuth service.

**Step 7** At the bottom of the browser window, click **Replicate Now**.

Cisco Secure ACS saves the replication configuration. Cisco Secure ACS immediately begins sending replicated database components to the secondary Cisco Secure ACSes you specified.



Downloaded from www.Manualslib.com manuals search engine

**Note** Replication only occurs when the database of the primary Cisco Secure ACS has changed since the last successful replication. You can force replication to occur by making one change to a user or group profile, such as changing a password or RADIUS attribute.

# Scheduling Replication

You can schedule when a primary Cisco Secure ACS sends its replicated database components to a secondary Cisco Secure ACS. For more information about replication scheduling options, see Outbound Replication Options, page 9-12.

**Note** Replication cannot occur until the secondary Cisco Secure ACSes are configured properly. For more information, see Configuring a Secondary Cisco Secure ACS, page 9-17.

### Before You Begin

Ensure correct configuration of the primary and secondary Cisco Secure ACSes. For detailed steps, see Implementing Primary and Secondary Replication Setups on Cisco Secure ACSes, page 9-15.

For each secondary Cisco Secure ACS of this primary Cisco Secure ACS, ensure that you have completed the steps in Configuring a Secondary Cisco Secure ACS, page 9-17.

To schedule when a primary Cisco Secure ACS replicates to its secondary Cisco Secure ACSes, follow these steps:

**Step 1** Log in to the HTML interface on the primary Cisco Secure ACS.

**Step 2** In the navigation bar, click **System Configuration**.

**Step 3** Click **CiscoSecure Database Replication**.



Downloaded from www.Manualslib.com manuals search engine

**Note** If this feature does not appear, click **Interface Configuration**, click Advanced Options, and select the **CiscoSecure ACS Database Replication** check box. Select the **Distributed System Settings** check box if not already selected.

The Database Replication Setup page appears.

**Step 4** To specify which CiscoSecure database components the primary Cisco Secure ACS should send to its secondary Cisco Secure ACSes, under Replication Components, select the corresponding **Send** check box for each database component to be sent.

For more information about replicated database components, see Replication Components Options, page 9-11.

**Step 5** To have the primary Cisco Secure ACS send replicated database components to its secondary Cisco Secure ACSes at regular intervals, under Replication Scheduling, select the **Every** *X* **minutes** option and in the *X* box type the length of the interval at which Cisco Secure ACS should perform replication (up to 7 characters).

**Note** Because Cisco Secure ACS is momentarily shut down during replication, a short replication interval may cause frequent failover of your AAA clients to other Cisco Secure ACSes. If AAA clients are not configured to failover to other Cisco Secure ACSes, the brief interruption in authentication service may prevent users from authenticating. For more information, see Replication Frequency, page 9-7.

**Step 6** If you want to schedule times at which the primary Cisco Secure ACS sends its replicated database components to its secondary Cisco Secure ACSes, follow these steps:

**a.** In the Outbound Replication table, select the **At specific times** option.

**b.** In the day and hour graph, click the times at which you want Cisco Secure ACS to perform replication.



Downloaded from www.Manualslib.com manuals search engine

**Tip** Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click Clear All to clear all hours, or you can click Set All to select all hours.

**Step 7** If you want to have this Cisco Secure ACS send replicated database components immediately upon receiving replicated database components from another Cisco Secure ACS, select the **Automatically triggered cascade** option.

**Note** If you specify the Automatically triggered cascade option, you must configure another Cisco Secure ACS to act as a primary Cisco Secure ACS to this Cisco Secure ACS; otherwise, this Cisco Secure ACS never replicates to its secondary Cisco Secure ACSes.

**Step 8** You must specify the secondary Cisco Secure ACSes that this Cisco Secure ACS should replicate to. To do so, follow these steps:

**Note** Cisco Secure ACS does not support bidirectional database replication. A secondary Cisco Secure ACS receiving replicated database components verifies that the primary Cisco Secure ACS is not on its Replication list. If not, the secondary Cisco Secure ACS accepts the replicated database components. If so, it rejects the components. For more information about replication partners, see Inbound Replication Options, page 9-15.

**a.** In the Outbound Replication table, from the AAA Servers list, select the name of a secondary Cisco Secure ACS to which you want the primary Cisco Secure ACS to send its selected replicated database components.

**Note** The secondary Cisco Secure ACSes available in the AAA Servers list are determined by the AAA Servers table in Network Configuration. For more information about the AAA Servers table, see AAA Server Configuration, page 4-21.

**b.** Click **-->** (right arrow button).

The selected secondary Cisco Secure ACS moves to the Replication list.



Downloaded from www.Manualslib.com manuals search engine

c. Repeat Step a and Step b for each secondary Cisco Secure ACS to which you want the primary Cisco Secure ACS to send its selected replicated database components.

**Step 9** In the **Replication timeout** text box, specify how long this Cisco Secure ACS will perform replication to each of its secondary Cisco Secure ACS before terminating the replication attempt and restarting the CSAuth service.

**Step 10** Click **Submit**.

Cisco Secure ACS saves the replication configuration you created.

# Disabling CiscoSecure Database Replication

You can disable scheduled CiscoSecure database replications without losing the schedule itself. This allows you to cease scheduled replications temporarily and later resume them without having to re-enter the schedule information.

To disable CiscoSecure database replication, follow these steps:

**Step 1** Log in to the HTML interface on the primary Cisco Secure ACS.

**Step 2** In the navigation bar, click **System Configuration**.

**Step 3** Click **CiscoSecure Database Replication**.

The Database Replication Setup page appears.

**Step 4** In the Replication Components table, clear all check boxes.

**Step 5** In the Outbound Replication table, select the **Manually** option.

**Step 6** Click **Submit**.

Cisco Secure ACS does not permit any replication to or from this Cisco Secure ACS server.



Downloaded from www.Manualslib.com manuals search engine

## Database Replication Event Errors

The Database Replication report contains messages indicating errors that occur during replication. For more information about the Database Replication report, see Cisco Secure ACS System Logs, page 11-13.

# RDBMS Synchronization

This section provides information about the RDBMS Synchronization feature, including procedures for implementing this feature, within both Cisco Secure ACS and the external data source involved.

This section contains the following topics:


- About RDBMS Synchronization, page 9-26
  - Users, page 9-27
  - User Groups, page 9-27
  - Network Configuration, page 9-28
  - Custom RADIUS Vendors and VSAs, page 9-28
- RDBMS Synchronization Components, page 9-29
  - About CSDBSync, page 9-29
  - About the accountActions Table, page 9-31
- Cisco Secure ACS Database Recovery Using the accountActions Table, page 9-32
- Reports and Event (Error) Handling, page 9-33
- Preparing to Use RDBMS Synchronization, page 9-33
- Considerations for Using CSV-Based Synchronization, page 9-35
  - Preparing for CSV-Based Synchronization, page 9-36
- Configuring a System Data Source Name for RDBMS Synchronization, page 9-37
- RDBMS Synchronization Options, page 9-38
  - RDBMS Setup Options, page 9-38
  - Synchronization Scheduling Options, page 9-39




Downloaded from www.Manualslib.com manuals search engine

– Synchronization Partners Options, page 9-39
- Performing RDBMS Synchronization Immediately, page 9-40
- Scheduling RDBMS Synchronization, page 9-41
- Disabling Scheduled RDBMS Synchronizations, page 9-43

# About RDBMS Synchronization

The RDBMS Synchronization feature enables you to update the CiscoSecure user database with information from an ODBC-compliant data source. The ODBC-compliant data source can be the RDBMS database of a third-party application. It can also be an intermediate file or database that a third-party system updates. Regardless of where the file or database resides, Cisco Secure ACS reads the file or database via the ODBC connection. You can also regard RDBMS Synchronization as an API—much of what you can configure for a user, group, or device through the Cisco Secure ACS HTML interface, you can alternatively maintain through this feature. RDBMS Synchronization supports addition, modification, and deletion for all data items it can access.

You can configure synchronization to occur on a regular schedule. You can also perform synchronizations manually, updating the CiscoSecure user database on demand.

Synchronization performed by a single Cisco Secure ACS can update the internal databases of other Cisco Secure ACSes, so that you only need configure RDBMS Synchronization on one Cisco Secure ACS. Cisco Secure ACSes listen on TCP port 2000 for synchronization data. RDBMS Synchronization communication between Cisco Secure ACSes is encrypted using 128-bit encrypted, proprietary algorithm.

The topics in this section provide an overview of the kinds of configuration that RDBMS Synchronization can automate. You specify the actions in a relational database table or text file named accountActions. For more information about accountActions, see About the accountActions Table, page 9-31. For specific information about all actions that RDBMS Synchronization can perform, see Appendix F, “RDBMS Synchronization Import Definitions”.



Downloaded from www.Manualslib.com manuals search engine

## Users

Among the user-related configuration actions that RDBMS Synchronization can perform are the following:

- Adding users.
- Deleting users.
- Setting passwords.
- Setting user group memberships.
- Setting Max Sessions parameters.
- Setting network usage quota parameters.
- Configuring command authorizations.
- Configuring network access restrictions.
- Configuring time-of-day/day-of-week access restrictions.
- Assigning IP addresses.
- Specifying outbound RADIUS attribute values.
- Specifying outbound TACACS+ attribute values.

**Note** For specific information about all actions that RDBMS Synchronization can perform, see Appendix F, "RDBMS Synchronization Import Definitions".

## User Groups

Among the group-related configuration actions that RDBMS Synchronization can perform are the following:

- Setting Max Sessions parameters.
- Setting network usage quota parameters.
- Configuring command authorizations.
- Configuring network access restrictions.
- Configuring time-of-day/day-of-week access restrictions.
- Specifying outbound RADIUS attribute values.



Downloaded from www.Manualslib.com manuals search engine

- Specifying outbound TACACS+ attribute values.

**Note** For specific information about all actions that RDBMS Synchronization can perform, see Appendix F, "RDBMS Synchronization Import Definitions".

## Network Configuration

Among the network device-related configuration actions that RDBMS Synchronization can perform are the following:

- Adding AAA clients.
- Deleting AAA clients.
- Setting AAA client configuration details.
- Adding AAA servers.
- Deleting AAA servers.
- Setting AAA server configuration details.
- Adding and configuring Proxy Distribution Table entries.

**Note** For specific information about all actions that RDBMS Synchronization can perform, see Appendix F, "RDBMS Synchronization Import Definitions".

## Custom RADIUS Vendors and VSAs

RDBMS Synchronization enables you to configure custom RADIUS vendors and VSAs. In addition to supporting a set of predefined RADIUS vendors and vendor-specific attributes (VSAs), Cisco Secure ACS supports RADIUS vendors and VSAs that you define. Vendors you add must be IETF-compliant; therefore, all VSAs that you add must be sub-attributes of IETF RADIUS attribute number 26.

You can define up to ten custom RADIUS vendors. Cisco Secure ACS allows only one instance of any given vendor, as defined by the unique vendor IETF ID number and by the vendor name.



Downloaded from www.Manualslib.com manuals search engine

**Note** If you intend to replicate user-defined RADIUS vendor and VSA configurations, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary Cisco Secure ACSes, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy. For more information about database replication, see CiscoSecure Database Replication, page 9-1.

For specific information about all actions that RDBMS Synchronization can perform, see Appendix F, "RDBMS Synchronization Import Definitions".

# RDBMS Synchronization Components

The RDBMS Synchronization feature comprises two components:

- **CSDBSync**—A dedicated Windows service that performs automated user and group account management services for Cisco Secure ACS.
- **accountActions Table**—The data object that holds information used by CSDBSync to update the CiscoSecure user database.

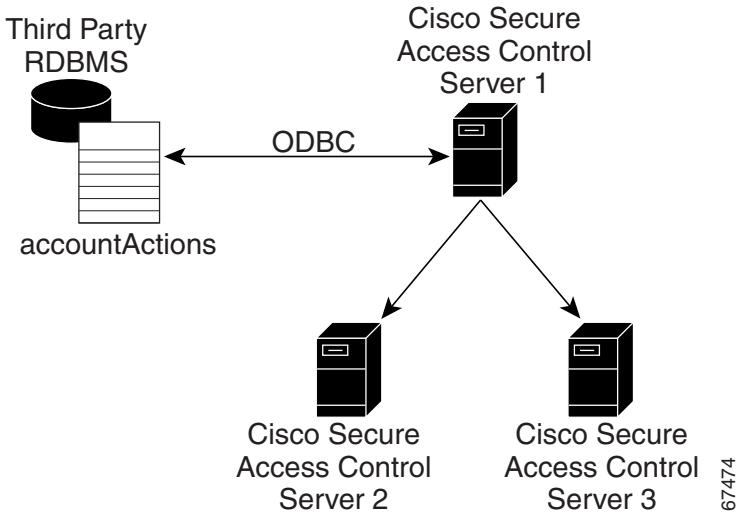
## About CSDBSync

The CSDBSync service uses an ODBC system data source name (DSN) to access the accountActions table. See Figure 9-2. This service looks specifically for a table named "accountActions". Synchronization events fail if CSDBSync cannot access the accountActions table.



Downloaded from www.Manualslib.com manuals search engine

*Figure 9-2 RDBMS Synchronization*




CSDBSync reads each record from the accountActions table and updates the CiscoSecure user database as specified by the action code in the record. For example, a record could instruct CSDBSync to add a user or change a user password. In a distributed environment, a single Cisco Secure ACS, known as the senior synchronization partner, accesses the accountActions table and sends synchronization commands to its synchronization partners. In Figure 9-2, Cisco Secure Access Control Server 1 is the senior synchronization partner and the other two Cisco Secure ACSes are its synchronization partners.

**Note** The senior synchronization partner must have AAA configurations for each Cisco Secure ACS that is a synchronization partners. In turn, each of the synchronization partners must have a AAA server configuration for the senior partner. Synchronization commands from the senior partner are ignored if the Cisco Secure ACS receiving the synchronization commands does not have a AAA server configuration for the senior partner.

CSDBSync both reads and writes (deletes records) in the accountActions table. After CSDBSync processes each record, it deletes the record from the table. This requires that the database user account that you configure the system DSN to use must have both read and write privileges.

For more information about CSDBSync or other Windows services used by Cisco Secure ACS, see Chapter 1, “Overview”.



Downloaded from www.Manualslib.com manuals search engine

## About the accountActions Table

The accountActions table contains a set of rows that define actions CSDBSync is to perform in the CiscoSecure user database. Each row in the accountActions table holds user, user group, or AAA client information. Each row also contains an action field and several other fields. These fields provide CSDBSync with the information it needs to update the CiscoSecure user database. For full details of the accountActions table format and available actions, see Appendix F, "RDBMS Synchronization Import Definitions".

The database containing the accountActions table must support a multi-threaded ODBC driver. This is required to prevent problems if Cisco Secure ACS and the third-party system attempt to access the accountActions table simultaneously.

Cisco Secure ACS includes files to help you create your accountActions table for several common formats. You can find these files on the Cisco Secure ACS in the following location, assuming a default installation of Cisco Secure ACS:

`C:\Program Files\CiscoSecure ACS v`*x.x*`\CSDBSync\Databases`

The Databases directory contains the following subdirectories:

- **Access**—Contains the file `CiscoSecure Transactions.mdb`.

  `CiscoSecure Transactions.mdb` contains a preconfigured accountActions table. When you install Cisco Secure ACS, the installation routine creates a system DSN named CiscoSecure DBSync. This system DSN is configured to communicate with `CiscoSecure Transactions.mdb`.

  **Note** By default, the username and password for the `CiscoSecure Transactions.mdb` database are set to null. To increase the security of RDBMS synchronizations performed using this database, change the username and password, both in the `CiscoSecure Transactions.mdb` database and in Cisco Secure ACS. Any other processes that access the `CiscoSecure Transactions.mdb` database should be changed to use the new username and password, too.

- **CSV**—Contains the files `accountactions` and `schema.ini`.

  The `accountactions` file is the accountActions table in a comma-separated value file. The `schema.ini` file provides the Microsoft ODBC text file driver with the information it needs to access the accountactions file.



Downloaded from www.Manualslib.com manuals search engine

- **Oracle 7**—Contains the files `accountActions.sql` and `testData.sql`.

  The `accountActions.sql` file contains the Oracle 7 SQL procedure needed to generate an accountActions table. The `testData.sql` file contains Oracle 7 SQL procedures for updating the accountActions table with sample transactions that CSDBSync can process.

- **Oracle 8**—Contains the files `accountActions.sql` and `testData.sql`.

  The `accountActions.sql` file contains the Oracle 8 SQL procedure needed to generate an accountActions table. The `testData.sql` file contains Oracle 8 SQL procedures for updating the accountActions table with sample transactions that CSDBSync can process.

- **SQL Server 6.5**—Contains the files `accountActions.sql` and `testData.sql`.

  The `accountActions.sql` file contains the Microsoft SQL Server 6.5 SQL procedure needed to generate an accountActions table. The `testData.sql` file contains Microsoft SQL Server 6.5 SQL procedures for updating the accountActions table with sample transactions that CSDBSync can process.

# Cisco Secure ACS Database Recovery Using the accountActions Table

Because the RDBMS Synchronization feature deletes each record in the accountActions table after processing the record, the accountActions table can be considered a transaction queue. The RDBMS Synchronization feature does not maintain a transaction log/audit trail. If a log is required, the external system that adds records to the accountActions table must create it. Unless the external system can recreate the entire transaction history in the accountActions table, we recommend that you construct a transaction log file for recovery purposes. To do this, create a second table that is stored in a safe location and backed up regularly. In that second table, mirror all the additions and updates to records in the accountActions table.

If the database is large, it is not practical to replay all transaction logs to synchronize the CiscoSecure user database with the third-party system. Instead, create regular backups of the CiscoSecure user database and replay the transaction logs from the time of most recent backup to bring the CiscoSecure user database back in synchronization with the third-party system. For information on creating backup files, see Cisco Secure ACS Backup, page 8-9.



Downloaded from www.Manualslib.com manuals search engine

Replaying transaction logs that slightly predate the checkpoint does not damage the CiscoSecure user database, although some transactions might be invalid and reported as errors. As long as the entire transaction log is replayed, the CiscoSecure user database is consistent with the database of the external RDBMS application.

# Reports and Event (Error) Handling

The CSDBSync service provides event and error logging. For more information about the RDBMS Synchronization log, see Cisco Secure ACS System Logs, page 11-13. For more information about the CSDBSync service log, see Service Logs, page 11-31.

During manual synchronizations, Cisco Secure ACS provides visual alerts to notify you of problems that occurred during synchronization.

# Preparing to Use RDBMS Synchronization

Synchronizing the CiscoSecure user database using data from the accountActions table requires that you complete several steps external to Cisco Secure ACS before you configure the RDBMS Synchronization feature within Cisco Secure ACS. If you are planning to use a CSV file as your accountActions table, also see Considerations for Using CSV-Based Synchronization, page 9-35.

To prepare to use RDBMS Synchronization, follow these steps:

**Step 1** Determine where you want to create the accountActions table and in what format. For more information about the accountActions table, see About the accountActions Table, page 9-31. For details on the format and content of the accountActions table, see Appendix F, "RDBMS Synchronization Import Definitions".

**Step 2** Create your accountActions table.

**Step 3** Configure your third-party system to generate records and update the accountActions table with them. This will most likely involve creating stored procedures that write to the accountActions table at a triggered event; however, the mechanism for maintaining your accountActions table is unique to your



Downloaded from www.Manualslib.com manuals search engine

implementation. If the third-party system you are using to update the accountActions table is a commercial product, for assistance, refer to the documentation supplied by your third-party system vendor.

For information about the format and content of the accountActions table, see Appendix F, "RDBMS Synchronization Import Definitions".

**Step 4** Validate that your third-party system updates the accountActions table properly. Rows generated in the accountActions table must be valid. For details on the format and content of the accountActions table, see Appendix F, "RDBMS Synchronization Import Definitions".

**Note** After testing that the third-party system updates the accountActions table properly, discontinue updating the accountActions table until after you have completed Step 6 and Step 7.

**Step 5** If you have a distributed AAA environment and want to synchronize multiple Cisco Secure ACSes, follow these steps:

a. Determine which Cisco Secure ACS you want to use to communicate with the third-party system. This is the senior synchronization partner, which you will later configure to send synchronization data to its synchronization partners, which are the other Cisco Secure ACSes needing synchronization.

b. On the senior synchronization partner, verify that there is a AAA server configuration for each synchronization partner. Add AAA server configuration for each missing synchronization partner. For detailed steps about adding a AAA server, see Adding a AAA Server, page 4-24.

c. On all the other synchronization partners, verify that there is a AAA server configuration for the senior synchronization partner. If no AAA server configuration for the senior synchronization partner exists, create one. For detailed steps about adding a AAA server, see Adding a AAA Server, page 4-24.

Synchronization between the senior synchronization partner and the other synchronization partners is enabled.

**Step 6** Set up a system DSN on the senior synchronization partner (the Cisco Secure ACS that will communicate with the third-party system). For steps, see Configuring a System Data Source Name for RDBMS Synchronization, page 9-37.



Downloaded from www.Manualslib.com manuals search engine

**Step 7** Schedule RDBMS synchronization on the senior synchronization partner. For steps, see Scheduling RDBMS Synchronization, page 9-41.

**Step 8** Configure your third-party system to begin updating the accountActions table with information to be imported into the CiscoSecure user database.

**Step 9** Confirm that RDBMS synchronization is operating properly by monitoring the RDBMS Synchronization report in the Reports and Activity section. For more information about the RDBMS Synchronization log, see Cisco Secure ACS System Logs, page 11-13.

Also, monitor the CSDBSync service log. For more information about the CSDBSync service log, see Service Logs, page 11-31.

# Considerations for Using CSV-Based Synchronization

The behavior of the Microsoft ODBC driver for text files creates additional considerations if you are planning to use a CSV-based accountActions table. The Microsoft ODBC driver for text files always operates in a read-only mode. It cannot delete records from a CSV accountActions table. Because of this, synchronization events initiated or scheduled in the HTML interface never release the CSV file, so the updates to the accountActions table from your third-party system fail.

The solution is to initiate synchronization events from a script, such as a DOS batch file. In the script, RDBMS synchronization is initiated with the **CSDBSync -run** command.

Assuming a default installation, CSDBSync.exe is installed at:

```
C:\Program Files\CiscoSecure ACS vx.x\CSDBSync
```

You can write a script that uses the CSDBsync command. You can schedule times when the script is run by using the Windows **at** command. For information about the **at** command, please refer to your Microsoft Windows documentation.

Also, due to limitations of the Microsoft ODBC text file driver, using the CSV format requires a change to the accountactions CSV file shipped with Cisco Secure ACS and to Cisco Secure ACS configuration. For more information, see Preparing for CSV-Based Synchronization, page 9-36.



Downloaded from www.Manualslib.com manuals search engine

# Preparing for CSV-Based Synchronization

If you want to use a CSV file for your accountActions table, some additional configuration is necessary. This is because the Microsoft ODBC CSV driver cannot access the accountActions table unless the file has a .csv file extension.

To prepare for RDBMS synchronization using a CSV file, follow these steps:

**Step 1** Rename the accountactions CSV file installed on the computer running Cisco Secure ACS to `accountactions.csv`.

Assuming a default installation of Cisco Secure ACS, the accountactions file is at the following location:

`C:\Program Files\CiscoSecure ACS v`*x.x*`\CSDBSync\Databases\CSV`

Where *x.x* refers to the version of your Cisco Secure ACS.

**Step 2** Edit the Windows Registry:

**a.** Access the following key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAAv`*x.x*`\CSDBSync`

**b.** Change the OdbcUpdateTable value from `AccountActions` to `accountactions.csv`.

**Note** You cannot perform synchronization using a relational database table rather than a CSV file when the OdbcUpdateTable value is `accountactions.csv`. To do so, you must change the OdbcUpdateTable value back to `AccountActions`.

**c.** Save your changes to the Registry.

Cisco Secure ACS is configured to perform CSV-based synchronization only, using a file named accountactions.csv.

**Step 3** At a DOS prompt, follow these steps:

**a.** Type:

```
net stop CSDBSync
```

and then press **Enter**.

**b.** Type:



Downloaded from www.Manualslib.com manuals search engine

```
net start CSDBSync
```

and then press **Enter**.

The Microsoft ODBC CSV driver can now access the accountActions CSV file properly.

# Configuring a System Data Source Name for RDBMS Synchronization

On the Cisco Secure ACS, a system DSN must exist for Cisco Secure ACS to access the accountActions table. If you plan to use the `CiscoSecure Transactions.mdb` Microsoft Access database provided with Cisco Secure ACS, you can use the `CiscoSecure DBSync` system DSN rather than create one.

For more information about the `CiscoSecure Transactions.mdb` file, see Preparing to Use RDBMS Synchronization, page 9-33.

To create a system DSN for use with RDBMS synchronization, follow these steps:

**Step 1** From Windows Control Panel, open the ODBC Data Source Administrator window.

**Tip** In Windows 2000, the ODBC Data Sources icon is located in the Administrative Tools folder.

**Step 2** In the ODBC Data Source Administrator window, click the **System DSN** tab.

**Step 3** Click **Add**.

**Step 4** Select the driver you need to use with your new DSN, and then click **Finish**.

A dialog box displays fields requiring information specific to the ODBC driver you selected.

**Step 5** In the Data Source Name box, type a descriptive name for the DSN.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** Complete the other fields required by the ODBC driver you selected. These fields may include information such as the IP address of the server on which the ODBC-compliant database runs.

**Step 7** Click **OK**.

The name you assigned to the DSN appears in the System Data Sources list.

**Step 8** Close the ODBC window and Windows Control Panel.

The system DSN to be used by Cisco Secure ACS to access your accountActions table is created on your Cisco Secure ACS.

# RDBMS Synchronization Options

The RDBMS Synchronization Setup page, available from System Configuration, provides control of the RDBMS Synchronization feature. It contains three tables whose options are described in this section.

This section contains the following topics:


- RDBMS Setup Options, page 9-38
- Synchronization Scheduling Options, page 9-39
- Synchronization Partners Options, page 9-39


## RDBMS Setup Options

The RDBMS Setup table defines how Cisco Secure ACS accesses the accountActions table. It contains the following options:

- **Data Source**—Specifies which of all the system DSNs available on the Cisco Secure ACS is to be used to access the accountActions table.
- **Username**—Specifies the username Cisco Secure ACS should use to access the database that contains the accountActions table.

**Note** The database user account specified by the username must have sufficient privileges to read and write to the accountActions table.



Downloaded from www.Manualslib.com manuals search engine

- **Password**—Specifies the password Cisco Secure ACS uses to access the database that contains the accountActions table.

## Synchronization Scheduling Options

The Synchronization Scheduling table defines when synchronization occurs. It contains the following scheduling options:

- **Manually**—Cisco Secure ACS does not perform automatic RDBMS synchronization.
- **Every *X* minutes**—Cisco Secure ACS performs synchronization on a set frequency. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times...**—Cisco Secure ACS performs synchronization at the time specified in the day and hour graph. The minimum interval is one hour, and the synchronization takes place on the hour selected.

## Synchronization Partners Options

The Synchronization Partners table defines which Cisco Secure ACSes are synchronized with data from the accountActions table. It provides the following options:

- **AAA Server**—This list represents the AAA servers configured in the AAA Servers table in Network Configuration for which the Cisco Secure ACS *does not* perform RDBMS synchronization.
- **Synchronize**—This list represents the AAA servers configured in the AAA Servers table in Network Configuration for which the Cisco Secure ACS *does* perform RDBMS synchronization. The AAA servers on this list are the synchronization partners of this Cisco Secure ACS. During synchronization, communication between this Cisco Secure ACS and its synchronization partners is 128-bit encrypted with a Cisco-proprietary protocol. The synchronization partners receive synchronization data on TCP port 2000.

**Note** Each synchronization partner *must* have a AAA server configuration in its Network Configuration section that corresponds to this Cisco Secure ACS; otherwise, the synchronization commands this Cisco Secure ACS sends to it are ignored.



Downloaded from www.Manualslib.com manuals search engine

For more information about the AAA Servers table in Network Configuration, see AAA Server Configuration, page 4-21.

# Performing RDBMS Synchronization Immediately

You can manually start an RDBMS synchronization event.

To perform manual RDBMS synchronization, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **RDBMS Synchronization**.

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **RDBMS Synchronization** check box.

The RDBMS Synchronization Setup page appears.

**Step 3** To specify options in the RDBMS Setup table, follow these steps:

**Note** For more information about RDBMS setup, see RDBMS Setup Options, page 9-38.

a. From the Data Source list, select the system DSN you configured to communicate with the database that contains your accountActions table.

   For more information about configuring a system DSN for use with RDBMS Synchronization, see Configuring a System Data Source Name for RDBMS Synchronization, page 9-37.

b. In the Username box, type the username for a database user account that has read/write access to the accountActions table.

c. In the Password box, type the password for the username specified in the Step b.

Cisco Secure ACS has the information necessary to access the accountActions table.



Downloaded from www.Manualslib.com manuals search engine

**Note** You do *not* have to select Manually under Replication Scheduling. For more information, see Disabling Scheduled RDBMS Synchronizations, page 9-43.

**Step 4** For each Cisco Secure ACS that you want this Cisco Secure ACS to update with data from the accountActions table, select the Cisco Secure ACS in the AAA Servers list, and then click **-->** (right arrow button).

The selected Cisco Secure ACS appears in the Synchronize list.

**Step 5** To remove Cisco Secure ACSes from the Synchronize list, select the Cisco Secure ACS in the Synchronize list, and then click **<--** (left arrow button).

The selected Cisco Secure ACS appears in the AAA Servers list.

**Step 6** At the bottom of the browser window, click **Synchronize Now**.

Cisco Secure ACS immediately begins a synchronization event. To check the status of the synchronization, view the RDBMS Synchronization report in Reports and Activity.

# Scheduling RDBMS Synchronization

You can schedule when a Cisco Secure ACS performs RDBMS synchronization.

To schedule when a Cisco Secure ACS performs RDBMS synchronization, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **RDBMS Synchronization**.

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **RDBMS Synchronization** check box.

The RDBMS Synchronization Setup page appears.

**Step 3** To specify options in the RDBMS Setup table, follow these steps:



Downloaded from www.Manualslib.com manuals search engine

**Note** For more information about RDBMS setup, see RDBMS Setup Options, page 9-38.

a. From the Data Source list, select the system DSN you configured to communicate with the database that contains your accountActions table.

   For more information about configuring a system DSN for use with RDBMS Synchronization, see Configuring a System Data Source Name for RDBMS Synchronization, page 9-37.

b. In the Username box, type the username for a database user account that has read/write access to the accountActions table.

c. In the Password box, type the password for the username specified in the Step b.

**Step 4** To have this Cisco Secure ACS perform RDBMS synchronization at regular intervals, under Synchronization Scheduling, select the **Every** *X* **minutes** option and in the *X* box type the length of the interval at which Cisco Secure ACS should perform synchronization (up to 7 characters).

**Step 5** To schedule times at which this Cisco Secure ACS performs RDBMS synchronization, follow these steps:

a. Under Synchronization Scheduling, select the **At specific times** option.

b. In the day and hour graph, click the times at which you want Cisco Secure ACS to perform replication.

**Tip** Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

**Step 6** For each Cisco Secure ACS you want to synchronize with data from the accountActions table, follow these steps:



Downloaded from www.Manualslib.com manuals search engine

**Note** For more information about synchronization targets, see Inbound Replication Options, page 9-15.

a. In the Synchronization Partners table, from the AAA Servers list, select the name of a Cisco Secure ACS that you want this Cisco Secure ACS to update with data from the accountActions table.

**Note** The Cisco Secure ACSes available in the AAA Servers list is determined by the AAA Servers table in Network Configuration, with the addition of the name of the current Cisco Secure ACS server. For more information about the AAA Servers table, see AAA Server Configuration, page 4-21.

b. Click **-->** (right arrow button).

The selected Cisco Secure ACS moves to the Synchronize list.

**Note** At least one Cisco Secure ACS must be in the Synchronize list. This includes the server on which you are configuring RDBMS Synchronization. RDBMS Synchronization does not automatically include the internal database of the current server.

**Step 7** Click **Submit**.

Cisco Secure ACS saves the RDBMS synchronization schedule you created.

# Disabling Scheduled RDBMS Synchronizations

You can disable scheduled RDBMS synchronization events without losing the schedule itself. This allows you to end scheduled synchronizations and resume them later without having to re-create the schedule.

To disable scheduled RDBMS synchronizations, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Click **RDBMS Synchronization**.

The RDBMS Synchronization Setup page appears.

**Step 3** Under Synchronization Scheduling, select the **Manually** option.

**Step 4** Click **Submit**.

Cisco Secure ACS does not perform scheduled RDBMS synchronizations.

# IP Pools Server

This section provides information about the IP Pools feature, including procedures for creating and maintaining IP pools.

This section contains the following topics:


- About IP Pools Server, page 9-44
- Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges, page 9-45
- Refreshing the AAA Server IP Pools Table, page 9-47
- Adding a New IP Pool, page 9-47
- Editing an IP Pool Definition, page 9-48
- Resetting an IP Pool, page 9-49
- Deleting an IP Pool, page 9-50


## About IP Pools Server

If you are using VPNs you may have to overlap IP address assignments; that is, it may be advantageous for a PPTP tunnel client within a given tunnel to use the same IP address as that used by another PPTP tunnel client in a different tunnel. The IP Pools Server feature enables you to assign the same IP address to multiple users, provided that the users are being tunnelled to different home gateways for routing beyond the boundaries of your own network. This means you can conserve your IP address space without having to resort to using illegal addresses. When



Downloaded from www.Manualslib.com manuals search engine

you enable this feature, Cisco Secure ACS dynamically issues IP addresses from the IP pools you have defined by number or name. You can configure up to 999 IP pools, for approximately 255,000 users.

If you are using IP pooling and proxy, all accounting packets are proxied so that the Cisco Secure ACS that is assigning the IP addresses can confirm whether an IP address is already in use.

**Note** IP pool definitions are not replicated by the CiscoSecure Database Replication feature; however, user and group assignments to IP pools are replicated. By not replicating IP pool definitions, Cisco Secure ACS avoids inadvertently assigning an IP address that a replication partner has already assigned to a different workstation. To support IP pools in a AAA environment that uses replication, you must manually configure each secondary Cisco Secure ACS to have IP pools with names identical to the IP pools defined on the primary Cisco Secure ACS.

To use IP pools, the AAA client must have network authorization (in IOS, **aaa authorization network**) and accounting (in IOS, **aaa accounting**) enabled.

**Note** To use the IP Pools feature, you must set up your AAA client to perform authentication and accounting using the same protocol—either TACACS+ or RADIUS.

For information on assigning a group or user to an IP pool, see Setting IP Address Assignment Method for a User Group, page 6-28 or Assigning a User to a Client IP Address, page 7-10.

# Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges

Cisco Secure ACS provides automated detection of overlapping pools.

**Note** To use overlapping pools, you must be using RADIUS with VPN, and you cannot be using Dynamic Host Configuration Protocol (DHCP).



Downloaded from www.Manualslib.com manuals search engine

You can determine whether overlapping IP pools are allowed by checking which button appears below the AAA Server IP Pools table:

- **Allow Overlapping Pool Address Ranges**—Indicates that overlapping IP pool address ranges are *not allowed*. Clicking this button allows IP address ranges to overlap between pools.
- **Force Unique Pool Address Range**—Indicates that overlapping IP pool address ranges are *allowed*. Clicking this button prevents IP address ranges from overlapping between pools.

To allow overlapping IP pools or to force unique pool address ranges, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **IP Pools Server**.

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **IP Pools** check box.

The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

**Step 3** If you want to allow overlapping IP pool address ranges, follow these steps:

**a.** If the Allow Overlapping Pool Address Ranges button appears, click that button.

Cisco Secure ACS allows overlapping IP pool address ranges.

**b.** If the Force Unique Pool Address Range button appears, do nothing.

Cisco Secure ACS already allows overlapping IP pool address ranges.

**Step 4** If you want to deny overlapping IP pool address ranges, follow these steps:

**a.** If the Allow Overlapping Pool Address Ranges button appears, do nothing.

Cisco Secure ACS already does not permit overlapping IP pool address ranges.

**b.** If the Force Unique Pool Address Range button appears, click that button.

Cisco Secure ACS does not permit overlapping IP pool address ranges.



Downloaded from www.Manualslib.com manuals search engine

# Refreshing the AAA Server IP Pools Table

You can refresh the AAA Server IP Pools table. This allows you to get the latest usage statistics for your IP pools.

To refresh the AAA Server IP Pools table, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

**Step 3** Click **Refresh**.

Cisco Secure ACS updates the percentages of pooled addresses in use.

# Adding a New IP Pool

You can define up to 999 IP address pools.

To add an IP pool, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools you have already configured, their address ranges, and the percentage of pooled addresses in use.

**Step 3** Click **Add Entry**.

The New Pool table appears.

**Step 4** In the Name box, type the name (up to 31 characters) you want to assign to the new IP pool.

**Step 5** In the Start Address box, type the lowest IP address (up to 15 characters) of the range of addresses for the new pool.



Downloaded from www.Manualslib.com manuals search engine

**Note** All addresses in an IP pool must be on the same Class C network, so the first three octets of the start and end addresses must be the same. For example, if the start address is 192.168.1.1, the end address must be between 192.168.1.2 and 192.168.1.254.

**Step 6** In the End Address box, type the highest IP address (up to 15 characters) of the range of addresses for the new pool.

**Step 7** Click **Submit**.

The new IP pool appears in the AAA Server IP Pools table.

# Editing an IP Pool Definition

To edit an IP pool definition, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

**Step 3** Click the name of the IP pool you need to edit.

The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use field displays how many IP addresses in this pool are allocated to a user. The Available field displays how many IP addresses are unallocated to users.

**Step 4** To change the name of the pool, in the Name box, type the name (up to 31 characters) to which you want to change the IP pool.

**Step 5** To change the starting address of the pool range of IP addresses, in the Start Address box, type the lowest IP address (up to 15 characters) of the new range of addresses for the pool.



Downloaded from www.Manualslib.com manuals search engine

**Note** All addresses in an IP pool must be on the same Class C network, so the first three octets of the start and end addresses must be the same. For example, if the start address is 192.168.1.1, the end address must be between 192.168.1.2 and 192.168.1.254.

**Step 6** To change the ending address of the pool range of IP addresses, in the End Address box, type the highest IP address (up to 15 characters) of the new range of addresses for the pool.

**Step 7** Click **Submit**.

The edited IP pool appears in the AAA Server IP Pools table.

# Resetting an IP Pool

The Reset function recovers IP addresses within an IP pool when there are "dangling" connections. A dangling connection occurs when a user disconnects and Cisco Secure ACS does not receive an accounting stop packet from the applicable AAA client. If the Failed Attempts log in Reports and Activity shows a large number of "Failed to Allocate IP Address For User" messages, consider using the Reset function to reclaim all allocated addresses in this IP pool.

**Note** Using the Reset function to reclaim all allocated IP addresses in a pool can result in users being assigned addresses that are already in use.

To reset an IP pool and reclaim all its IP addresses, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

**Step 3** Click the name of the IP pool you need to reset.



Downloaded from www.Manualslib.com manuals search engine

The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use field displays how many IP addresses in this pool are assigned to a user. The Available field displays how many IP addresses are not assigned to users.

**Step 4** Click **Reset**.

Cisco Secure ACS displays a dialog box indicating the possibility of assigning user addresses that are already in use.

**Step 5** To continue resetting the IP pool, click **OK**.

The IP pool is reset. All its IP addresses are reclaimed. In the In Use column of the AAA Server IP Pools table, zero percent of the IP pool addresses are assigned to users.

# Deleting an IP Pool

**Note** If you delete an IP pool that has users assigned to it, those users cannot authenticate until you edit the user profile and change their IP assignment settings. Alternatively, if the users receive their IP assignment based on group membership, you can edit the user group profile and change the IP assignment settings for the group.

To delete an IP pool, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

**Step 3** Click the name of the IP pool you need to delete.

The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use column displays how many IP addresses in this pool are assigned to a user. The Available column displays how many IP addresses are not assigned to users.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** Click **Delete**.

Cisco Secure ACS displays a dialog box to confirm that you want to delete the IP pool.

**Step 5** To delete the IP pool, click **OK**.

The IP pool is deleted. The AAA Server IP Pools table does not list the deleted IP pool.

# IP Pools Address Recovery

The IP Pools Address Recovery feature enables you to recover assigned IP addresses that have not been used for a specified period of time. You must configure an accounting network on the AAA client for Cisco Secure ACS to reclaim the IP addresses correctly.

## Enabling IP Pool Address Recovery

To enable IP pool address recovery, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **IP Pools Address Recovery**.

**Note** If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **IP Pools** check box.

The IP Address Recovery page appears.

**Step 3** Select the **Release address if allocated for longer than** *X* **hours** check box and in the *X* box type the number of hours (up to 4 characters) after which Cisco Secure ACS should recover assigned, unused IP addresses.

**Step 4** Click **Submit**.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS implements the IP pools address recovery settings you made.



Downloaded from www.Manualslib.com manuals search engine

CHAPTER 10

# System Configuration: Authentication and Certificates

This chapter addresses authentication and certification features found in the System Configuration section of Cisco Secure ACS Solution Engine.

This chapter contains the following topics:


- About Certification and EAP Protocols, page 10-1
- Global Authentication Setup, page 10-26
- Cisco Secure ACS Certificate Setup, page 10-34


## About Certification and EAP Protocols

Cisco Secure ACS uses EAP-TLS and PEAP authentication protocols in combination with digital certification to ensure the protection and validity of authentication information. Digital certification, EAP-TLS, PEAP, and machine authentication are described in the topics that follow.

This section contains the following topics:


- Digital Certificates, page 10-2
- EAP-TLS Authentication, page 10-2
- PEAP Authentication, page 10-8
- EAP-FAST Authentication, page 10-13





Downloaded from www.Manualslib.com manuals search engine

# Digital Certificates

The ACS Certificate Setup pages enable you to install digital certificates to support EAP-TLS and PEAP authentication, as well as to support HTTPS protocol for secure access to the Cisco Secure ACS HTML interface. Cisco Secure ACS uses the X.509 v3 digital certificate standard. Certificate files must be in either Base64-encoded X.509 format or DER-encoded binary X.509 format. Also, Cisco Secure ACS supports manual certificate enrollment and provides the means for managing a certificate trust list (CTL) and certificate revocation lists (CRL).

Digital certificates do not require the sharing of secrets or stored database credentials. They can be scaled and trusted over large deployments. If managed properly, they can serve as a method of authentication that is stronger and more secure than shared secret systems. Mutual trust requires that Cisco Secure ACS have an installed certificate that can be verified by end-user clients. This server certificate may be issued from a certification authority (CA) or, if you choose, may be a self-signed certificate. For more information seeInstalling a Cisco Secure ACS Server Certificate, page 10-35, and Using Self-Signed Certificates, page 10-47.

**Note** Depending on the end-user client involved, the CA certificate for the CA that issued the Cisco Secure ACS server certificate is likely to be required in local storage for trusted root CAs on the end-user client computer.

# EAP-TLS Authentication

This section contains the following topics:


- About the EAP-TLS Protocol, page 10-3
- EAP-TLS and Cisco Secure ACS, page 10-4
- EAP-TLS Limitations, page 10-6
- Enabling EAP-TLS Authentication, page 10-7




Downloaded from www.Manualslib.com manuals search engine

## About the EAP-TLS Protocol

EAP and TLS are both IETF RFC standards. The EAP protocol carries initial authentication information, specifically EAPOL (the encapsulation of EAP over LANs as established by IEEE 802.1X). TLS uses certificates both for user authentication and for dynamic ephemeral session key generation. The EAP-TLS authentication protocol uses the certificates of Cisco Secure ACS and of the end-user client, enforcing mutual authentication of the client and of Cisco Secure ACS. For more detailed information on EAP, TLS, and EAP-TLS, refer to the following IETF RFCs: PPP Extensible Authentication Protocol (EAP) RFC 2284, The TLS Protocol RFC 2246, and PPP EAP TLS Authentication Protocol RFC 2716.

EAP-TLS authentication involves two elements of trust. The first element of trust is when the EAP-TLS negotiation establishes end-user trust by validating, through RSA signature verifications, that the user possesses a keypair signed by a certificate. This verifies that the end user is the legitimate keyholder for a given digital certificate and the corresponding user identification contained in the certificate. However, trusting that a user possesses a certificate only provides a username/keypair binding. The second element of trust is to use a third-party signature, usually from a certification authority (CA), that verifies the information in a certificate. This third-party binding is similar to the real world equivalent of the seal on a passport. You trust the passport because you trust the preparation and identity checking that the particular country's passport office made when creating that passport. You trust digital certificates by installing the root certificate CA signature.

Some situations do not require this "second element of trust" that is provided by installing the root certificate CA signature. When such external validation of certificate legitimacy is not required, you can use the Cisco Secure ACS self-signed certificate capability. Depending on the end-user client involved, the CA certificate for the CA that issued the Cisco Secure ACS server certificate is likely to be required in local storage for trusted root CAs on the end-user client computer. For more information, see About Self-Signed Certificates, page 10-47.

EAP-TLS requires support from both the end client and the AAA client. An example of an EAP-TLS client includes the Microsoft Windows XP operating system; EAP-TLS-compliant AAA clients include Cisco 802.1x-enabled switch platforms (such as the Catalyst 6500 product line) and Cisco Aironet Wireless solutions. To accomplish secure Cisco Aironet connectivity, EAP-TLS generates a dynamic, per-user, per-connection, unique session key.



Downloaded from www.Manualslib.com manuals search engine

# EAP-TLS and Cisco Secure ACS

Cisco Secure ACS supports EAP-TLS with any end-user client that supports EAP-TLS, such as Windows XP. To learn which user databases support EAP-TLS, see Authentication Protocol-Database Compatibility, page 1-10. For more information about deploying EAP-TLS authentication, see *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks* at http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/acstl_wp.htm.

Cisco Secure ACS can use EAP-TLS to support machine authentication to Microsoft Windows Active Directory. The end-user client may limit the protocol used for user authentication to the same protocol used for machine authentication; that is, use of EAP-TLS for machine authentication may require the use of EAP-TLS for user authentication. For more information about machine authentication, see Machine Authentication, page 13-16.

Cisco Secure ACS supports domain stripping for EAP-TLS authentication using Windows Active Directory. For more information, see EAP-TLS Domain Stripping, page 13-16.

Cisco Secure ACS also supports three methods of certificate comparison and a session resume feature. This topic discusses these features.

To permit access to the network by a user or computer authenticating with EAP-TLS, Cisco Secure ACS must verify that the claimed identity (presented in the EAP Identity response) corresponds to the certificate presented by the user. Cisco Secure ACS can accomplish this verification in three ways:

- **Certificate SAN Comparison**—Based on the name in the Subject Alternative Name field in the user certificate.
- **Certificate CN Comparison**—Based on the name in the Subject Common Name field in the user certificate.
- **Certificate Binary Comparison**—Based on a binary comparison between the user certificate stored in the user object in the LDAP server or Active Directory and the certificate presented by the user during EAP-TLS authentication. This comparison method cannot be used to authenticate users stored in an ODBC external user database.



Downloaded from www.Manualslib.com manuals search engine

**Note** If you use certificate binary comparison, the user certificate must be stored in a binary format. Also, for generic LDAP and Active Directory, the attribute storing the certificate must be the standard LDAP attribute named "usercertificate".

When you set up EAP-TLS, you can select the criterion (one, two, or all) that Cisco Secure ACS uses. For more information, see Configuring Authentication Options, page 10-33.

Cisco Secure ACS supports a session resume feature for EAP-TLS-authenticated user sessions, a particularly useful feature for WLANs, wherein a user may move the client computer so that a different wireless access point is in use. When this feature is enabled, Cisco Secure ACS caches the TLS session created during EAP-TLS authentication, provided that the user successfully authenticates. If a user needs to reconnect and the original EAP-TLS session has not timed out, Cisco Secure ACS uses the cached TLS session, resulting in faster EAP-TLS performance and lessened AAA server load. When Cisco Secure ACS resumes an EAP-TLS session, the user reauthenticates by SSL handshake only, without a certificate comparison.

In effect, enabling EAP-TLS session resume allows Cisco Secure ACS to trust a user based on the cached TLS session from the original EAP-TLS authentication. Because Cisco Secure ACS only caches a TLS session when a new EAP-TLS authentication succeeds, the existence of a cached TLS session is proof that the user has successfully authenticated within the number of minutes defined by the EAP-TLS session timeout option.

**Note** Session timeout is based on the time of the initial, full authentication of the session. It is not dependent upon an accounting start message.

Changes to group assignment in an external user database are not enforced by the session resume feature. This is because group mapping does not occur when a user session is resumed. Instead, the user is mapped to the same Cisco Secure ACS group that the user was mapped to upon the beginning of the session. Upon the start of a new session, group mapping enforces the new group assignment.



Downloaded from www.Manualslib.com manuals search engine

To force an EAP-TLS session to end before the session timeout is reached, either restart the CSAuth service or delete the user from the CiscoSecure user database CiscoSecure user database. Disabling or deleting the user in an external user database has no effect because the session resume feature does not involve the use of external user databases.

You can enable the EAP-TLS session resume feature and configure the timeout interval on the Global Authentication Setup page. For more information about enabling this feature, see Global Authentication Setup, page 10-26.

## EAP-TLS Limitations

The Cisco Secure ACS implementation of EAP-TLS has the following limitations:

- **Server and CA certificate file format**—If you install the Cisco Secure ACS server and CA certificates from files rather than from certificate storage, server and CA certificate files must be in either Base64-encoded X.509 format or DER-encoded binary X.509 format.
- **LDAP attribute for binary comparison**—If you configure Cisco Secure ACS to perform binary comparison of user certificates, the user certificate must be stored in Active Directory or an LDAP server, using a binary format. Also, the attribute storing the certificate must be named “usercertificate”.
- **Windows server type**—If you want to use Active Directory to authenticate users with EAP-TLS when Cisco Secure ACS runs on a member server, additional configuration is required. For more information, including steps for the additional configuration, see *Installation Guide for Cisco Secure ACS for Windows Server.*

Additionally, if Cisco Secure ACS receives traffic from a wireless access point that has the wrong shared secret, the error message logged in the failed attempts log reads “EAP request has invalid signature”. Three conditions that might cause this to occur are the following:

- The wrong signature is being used.
- A RADIUS packet was corrupted in transit.
- Cisco Secure ACS is being attacked.



Downloaded from www.Manualslib.com manuals search engine

# Enabling EAP-TLS Authentication

This procedure provides an overview of the detailed procedures required to configure Cisco Secure ACS to support EAP-TLS authentication.

**Note** End-user client computers must be configured to support EAP-TLS. This procedure is specific to configuration of Cisco Secure ACS only. For more information about deploying EAP-TLS authentication, see *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks* at http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/acstl_wp.htm.

### Before You Begin

For EAP-TLS machine authentication, if you have a Microsoft certification authority server configured on the domain controller, you can configure a policy in Active Directory to produce a client certificate automatically when a computer is added to the domain. For more information, see Microsoft Knowledge Base Article 313407, HOW TO: Create Automatic Certificate Requests with Group Policy in Windows.

To enable EAP-TLS authentication, follow these steps:

**Step 1** Install a server certificate in Cisco Secure ACS. EAP-TLS requires a server certificate. For detailed steps, see Installing a Cisco Secure ACS Server Certificate, page 10-35.

**Note** If you have previously installed a certificate to support EAP-TLS or PEAP user authentication or to support HTTPS protection of remote Cisco Secure ACS administration, you do not need to perform this step. A single server certificate is sufficient to support all certificate-based Cisco Secure ACS services and remote administration; however, EAP-TLS and PEAP require that the certificate be suitable for server authentication purposes.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Edit the certification trust list so that the certification authority (CA) issuing end-user client certificates is trusted. If you do not perform this step, Cisco Secure ACS only trusts user certificates issued by the same CA that issued the certificate installed in Cisco Secure ACS. For detailed steps, see Editing the Certificate Trust List, page 10-38.

**Step 3** Establish a certificate revocation list (CRL) for each CA and certificate type listed in the certificate trust list (CTL). As part of EAP-TLS authentication, Cisco Secure ACS validates the status of the certificate presented by the user against the cached CRL to ensure that it has not been revoked. For detailed steps, see Adding a Certificate Revocation List Issuer, page 10-42.

**Step 4** Enable EAP-TLS on the Global Authentication Setup page. Cisco Secure ACS allows you to complete this step only after you have successfully completed Step 1. For detailed steps, see Configuring Authentication Options, page 10-33.

**Step 5** Configure a user database. To determine which user databases support EAP-TLS authentication, see Authentication Protocol-Database Compatibility, page 1-10.

Cisco Secure ACS is ready to perform EAP-TLS authentication.

# PEAP Authentication

This section contains the following topics:


- About the PEAP Protocol, page 10-8
- PEAP and Cisco Secure ACS, page 10-9
- PEAP and the Unknown User Policy, page 10-11
- Enabling PEAP Authentication, page 10-12


## About the PEAP Protocol

The PEAP (Protected EAP) protocol is a client-server security architecture that provides a means of encrypting EAP transactions, thereby protecting the contents of EAP authentications. PEAP has been posted as an IETF Internet Draft by RSA, Cisco, and Microsoft and is available at http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-05.txt.



Downloaded from www.Manualslib.com manuals search engine

PEAP authentications always involve two phases. In the first phase, the end-user client authenticates Cisco Secure ACS. This requires a server certificate and authenticates Cisco Secure ACS to the end-user client, ensuring that the user or machine credentials sent in phase two are sent to a AAA server that has a certificate issued by a trusted CA. The first phase uses a TLS handshake to establish an SSL tunnel.

**Note** Depending on the end-user client involved, the CA certificate for the CA that issued the Cisco Secure ACS server certificate is likely to be required in local storage for trusted root CAs on the end-user client computer.

In phase two, Cisco Secure ACS authenticates the user or machine credentials using an EAP authentication protocol. The EAP authentication is protected by the SSL tunnel created in phase one. The authentication type negotiated during the second conversation may be any valid EAP type, such as EAP-GTC (for Generic Token Card). Because PEAP can support any EAP authentication protocol, individual combinations of PEAP and EAP protocols are denoted with the EAP protocol within parentheses, such as PEAP(EAP-GTC). For the authentication protocols that Cisco Secure ACS supports in phase two of PEAP, see Authentication Protocol-Database Compatibility, page 1-10.

One improvement in security offered by PEAP is identity protection. This is the potential of protecting the username in all PEAP transactions. After phase one of PEAP, all data is encrypted, including username information usually sent in clear text. The Cisco Aironet PEAP client sends user identity through the SSL tunnel only. The initial identity, used in phase one and which is sent in the clear, is the MAC address of the end-user client with “PEAP_” as a prefix. The Microsoft PEAP client does not provide identity protection; the Microsoft PEAP client sends the username in the clear in phase one of PEAP authentication.

## PEAP and Cisco Secure ACS

Cisco Secure ACS supports PEAP authentication using either the Cisco Aironet PEAP client or the Microsoft PEAP client included with Microsoft Windows XP Service Pack 1. Cisco Secure ACS can support the Cisco Aironet PEAP client with PEAP(EAP-GTC) only. For the Microsoft PEAP client included with Windows XP Service Pack 1, Cisco Secure ACS supports only PEAP(EAP-MSCHAPv2). For information about which user databases support PEAP protocols, see Authentication Protocol-Database Compatibility, page 1-10.



Downloaded from www.Manualslib.com manuals search engine

When the end-user client is the Cisco Aironet PEAP client and both PEAP(EAP-GTC) and PEAP(EAP-MSCHAPv2) are enabled on the Global Authentication Setup page, Cisco Secure ACS first attempts PEAP(EAP-GTC) authentication with the end-user client. If the client rejects this protocol (by sending an EAP NAK message), Cisco Secure ACS attempts authentication with PEAP(EAP-MSCHAPv2). For more information about enabling EAP protocols supported within PEAP, see Global Authentication Setup, page 10-26.

Cisco Secure ACS can use PEAP(EAP-MSCHAPv2) to support machine authentication to Microsoft Windows Active Directory. The end-user client may limit the protocol used for user authentication to the same protocol used for machine authentication; that is, use of PEAP for machine authentication requires the use of PEAP for user authentication. For more information about machine authentication, see Machine Authentication, page 13-16.

Cisco Secure ACS supports a session resume feature for PEAP-authenticated user sessions. When this feature is enabled, Cisco Secure ACS caches the TLS session created during phase one of PEAP authentication, provided that the user successfully authenticates in phase two of PEAP. If a user needs to reconnect and the original PEAP session has not timed out, Cisco Secure ACS uses the cached TLS session, resulting in faster PEAP performance and lessened AAA server load.

**Note** Session timeout is based on the time that authentication succeeds. It is not dependent upon accounting.

You can enable the PEAP session resume feature and configure the timeout interval on the Global Authentication Setup page. For more information about enabling this feature, see Global Authentication Setup, page 10-26.

Cisco Secure ACS also supports a fast reconnect feature. When the session resume feature is enabled, the fast reconnection feature causes Cisco Secure ACS to allow a PEAP session to resume without checking user credentials. In effect, enabling this feature allows Cisco Secure ACS to trust a user based on the cached TLS session from the original PEAP authentication. Because Cisco Secure ACS only caches a TLS session when phase two of PEAP authentication succeeds, the existence of a cached TLS session is proof that the user has successfully authenticated within the number of minutes defined by the PEAP session timeout option.



Downloaded from www.Manualslib.com manuals search engine

Changes to group assignment in an external user database are not enforced by the session resume feature. This is because group mapping does not occur when a user session is extended by the session resume feature. Instead, the user is mapped to the same Cisco Secure ACS group that the user was mapped to upon the beginning of the session. Upon the start of a new session, group mapping enforces the new group assignment.

The fast reconnect feature is particularly useful for wireless LANs, wherein a user may move the client computer so that a different wireless access point is in use. When Cisco Secure ACS resumes a PEAP session, the user reauthenticates without entering a password, provided that the session has not timed out. If the end-user client is restarted, the user must enter a password even if the session timeout interval has not ended.

You can enable the PEAP fast reconnect feature on the Global Authentication Setup page. For more information about enabling this feature, see Global Authentication Setup, page 10-26.

## PEAP and the Unknown User Policy

During PEAP authentication, the real username to be authenticated may not be known by Cisco Secure ACS until phase two of authentication. While the Microsoft PEAP client does reveal the actual username during phase one, the Cisco PEAP client does not; therefore, Cisco Secure ACS does not attempt to look up the username presented during phase one and the use of the Unknown User Policy is irrelevant during phase one, regardless of the PEAP client used.

When phase two of PEAP authentication occurs and the username presented by the PEAP client is unknown to Cisco Secure ACS, Cisco Secure ACS processes the username in the same way that it processes usernames presented in other authentication protocols. If the username is unknown and the Unknown User Policy is disabled, authentication fails. If the username is unknown and the Unknown User Policy is enabled, Cisco Secure ACS attempts to authenticate the PEAP user with unknown user processing.

For more information about unknown user processing, see About Unknown User Authentication, page 15-4.



Downloaded from www.Manualslib.com manuals search engine

# Enabling PEAP Authentication

This procedure provides an overview of the detailed procedures required to configure Cisco Secure ACS to support PEAP authentication.

**Note** End-user client computers must be configured to support PEAP. This procedure is specific to configuration of Cisco Secure ACS only.

To enable PEAP authentication, follow these steps:

**Step 1** Install a server certificate in Cisco Secure ACS. PEAP requires a server certificate. For detailed steps, see Installing a Cisco Secure ACS Server Certificate, page 10-35.

**Note** If you have previously installed a certificate to support EAP-TLS or PEAP user authentication or to support HTTPS protection of remote Cisco Secure ACS administration, you do not need to perform this step. A single server certificate is sufficient to support all certificate-based Cisco Secure ACS services and remote administration; however, EAP-TLS and PEAP require that the certificate be suitable for server authentication purposes.

**Step 2** Enable PEAP on the Global Authentication Setup page. Cisco Secure ACS allows you to complete this step only after you have successfully completed Step 1. For detailed steps, see Configuring Authentication Options, page 10-33.

**Step 3** Configure a user database. To determine which user databases support PEAP authentication, see Authentication Protocol-Database Compatibility, page 1-10.

Cisco Secure ACS is ready to perform PEAP authentication for most users. For more information, see PEAP and the Unknown User Policy, page 10-11.

**Step 4** Consider enabling the Unknown User Policy to simplify PEAP authentication. For more information, see PEAP and the Unknown User Policy, page 10-11. For detailed steps, see Configuring the Unknown User Policy, page 15-16.



Downloaded from www.Manualslib.com manuals search engine

# EAP-FAST Authentication

This section contains the following topics:


- About EAP-FAST, page 10-13
- About Master Keys, page 10-15
- About PACs, page 10-17
  - Automatic PAC Provisioning, page 10-18
  - Manual PAC Provisioning, page 10-20
- Master Key and PAC TTLs, page 10-21
- Table 10-2
- Enabling EAP-FAST, page 10-25


## About EAP-FAST

The EAP Flexible Authentication via Secured Tunnel (EAP-FAST) protocol is a client-server security architecture that encrypts EAP transactions with a TLS tunnel. While similar to PEAP in this respect, it differs significantly in that EAP-FAST tunnel establishment is based upon strong secrets that are unique to users. These secrets are called Protected Access Credentials (PACs), which Cisco Secure ACS generates using a master key known only to Cisco Secure ACS. Because handshakes based upon shared secrets are intrinsically faster than handshakes based upon PKI, EAP-FAST is the significantly faster of the two solutions that provide encrypted EAP transactions. No certificate management is required to implement EAP-FAST.

EAP-FAST occurs in three phases:

- **Phase zero**—Unique to EAP-FAST, phase zero is a tunnel-secured means of providing an EAP-FAST end-user client with a PAC for the user requesting network access (see Automatic PAC Provisioning, page 10-18). Providing a PAC to the end-user client is the sole purpose of phase zero. The tunnel is established based on an anonymous Diffie-Hellman key exchange. If EAP-MSCHAPv2 authentication succeeds, Cisco Secure ACS provides the user a PAC. To determine which databases support EAP-FAST phase zero, see Authentication Protocol-Database Compatibility, page 1-10.



Downloaded from www.Manualslib.com manuals search engine

**Note** Phase zero is optional and PACs can be manually provided to end-user clients (see Manual PAC Provisioning, page 10-20). You control whether Cisco Secure ACS supports phase zero by selecting the Allow automatic PAC provisioning check box in the Global Authentication Configuration page.

No network service is enabled by phase zero of EAP-FAST; therefore, even a successful EAP-FAST phase zero transaction is recorded in the Cisco Secure ACS Failed Attempts log.

- **Phase one**—In phase one, Cisco Secure ACS and the end-user client establish a TLS tunnel based upon the PAC presented by the end-user client. This requires that the end-user client has been provided a PAC for the user attempting to gain network access and that the PAC is based on a master key that has not expired. The means by which PAC provisioning has occurred is irrelevant; either automatic or manual provisioning may be used.

  No network service is enabled by phase one of EAP-FAST.

- **Phase two**—In phase two, Cisco Secure ACS authenticates the user credentials with EAP-GTC, which is protected by the TLS tunnel created in phase one. No other EAP types are supported for EAP-FAST. To determine which databases support EAP-FAST phase two, see Authentication Protocol-Database Compatibility, page 1-10.

  Cisco Secure ACS authorizes network service with a successful user authentication in phase two of EAP-FAST and logs the authentication in the Passed Authentications log, if it is enabled. Also, if necessary, Cisco Secure ACS may refresh the end-user client PAC, which creates a second entry in the Passed Authentication log for the same phase two transaction.

EAP-FAST can protect the username in all EAP-FAST transactions. Cisco Secure ACS does not perform user authentication based on a username presented in phase one; however, whether the username is protected during phase one depends upon the end-user client. If the end-user client does not send the real username in phase one, the username is protected. The Cisco Aironet EAP-FAST client protects the username in phase one by sending `FAST_`*MAC address* in place of the username. After phase one of EAP-FAST, all data is encrypted, including username information usually sent in clear text.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS supports password aging with EAP-FAST for users authenticated by Windows user databases. Password aging can work with either phase zero or phase two of EAP-FAST. If password aging requires a user to change passwords during phase zero, the new password would be effective in phase two. For more information about password aging for Windows user databases, see Enabling Password Aging for Users in Windows Databases, page 6-26.

## About Master Keys

EAP-FAST master keys are strong secrets that Cisco Secure ACS automatically generates and that only Cisco Secure ACS is aware of. Master keys are never sent to an end-user client. EAP-FAST requires master keys for two purposes:

- **PAC generation**—Cisco Secure ACS generates PACs using the active master key. For details about PACs, see About PACs, page 10-17.
- **EAP-FAST phase one**—Cisco Secure ACS determines whether the PAC presented by the end-user client was generated by one of the master keys it is aware of, either the active master key or a retired master key.

To increase the security of EAP-FAST, Cisco Secure ACS changes the master key that it uses to generate PACs. Cisco Secure ACS uses time-to-live (TTL) values you define to determine when it generates a new master key and to determine the age of all master keys. Based on TTL values, Cisco Secure ACS assigns master keys one of the three following states:

- **Active**—An active master key is the master key used by Cisco Secure ACS to generate PACs. The duration that a master key remains active is determined by the Master key TTL setting. At any time, only one master key is active. When you define TTLs for master keys and PACs, Cisco Secure ACS permits only a PAC TTL that is shorter than the active master key TTL. This limitation ensures that a PAC is refreshed at least once before the expiration of the master key used to generate the PAC, provided that EAP-FAST users log in to the network at least once before the master key expires. For more information about how TTL values determine whether PAC refreshing or provisioning is required, see Master Key and PAC TTLs, page 10-21.

  When Cisco Secure ACS is configured to receive replicated EAP-FAST policies and master keys, a backup master key is among the master keys received. The backup master key is used only if the active master key retires



Downloaded from www.Manualslib.com manuals search engine

before the next successful master key replication. If the backup master key also retires before the next successful master key replication, EAP-FAST authentication fails for all users requesting network access with EAP-FAST.

**Tip** If EAP-FAST authentication fails because the active and backup master keys have retired and Cisco Secure ACS has not received new master keys in replication, you can force Cisco Secure ACS to generate its own master keys by selecting the EAP-FAST Master Server check box and clicking Submit.

Cisco Secure ACS records the generation of master keys in the logs for the CSAuth service.

- **Retired**—When a master key becomes older than the Master key TTL settings, it is considered retired for as long as specified by the Retired master key TTL settings. Cisco Secure ACS can store up to 255 retired master keys. While a retired master key is not used to generate new PACs, Cisco Secure ACS needs it to authenticate PACs that were generated using it. When you define TTLs for master keys and retired master keys, Cisco Secure ACS permits only TTL settings that require storing 255 or fewer retired master keys. For example, if the master key TTL is 1 hour and the retired master key TTL is 4 weeks, this would require storing up to 671 retired master keys; therefore, Cisco Secure ACS presents an error message and does not allow these settings.

  When a user gains network access using a PAC generated with a retired master key, Cisco Secure ACS provides the end-user client a new PAC generated with the active master key. For more information about Cisco Secure ACS with respect to the states of master keys and PACs, see Master Key and PAC TTLs, page 10-21.

- **Expired**—When a master key becomes older than the sum of the master key TTL and retired master TTL settings, it is considered expired and Cisco Secure ACS deletes it from its records of master keys. For example, if the master key TTL is one hour and the retired master key TTL is one week, a master key expires when it becomes greater than one week and one hour old.

  PACs generated by an expired master key cannot be used to access your network. An end-user client presenting a PAC that was generated with an expired master key must be provided a new PAC using automatic or manual provisioning before phase one of EAP-FAST can succeed.



Downloaded from www.Manualslib.com manuals search engine

# About PACs

PACs are strong shared secrets that enable Cisco Secure ACS and an EAP-FAST end-user client to authenticate each other and establish a TLS tunnel for use in EAP-FAST phase two. Cisco Secure ACS generates PACs using the active master key and a username. An EAP-FAST end-user client stores PACs for each user accessing the network with the client. Additionally, a AAA server that supports EAP-FAST has a unique Authority ID. An end-user client associates a user's PACs with the Authority ID of the AAA server that generated them.

During EAP-FAST phase one, the end-user client presents the PAC that it has for the current user and for the Authority ID sent by Cisco Secure ACS at the beginning of the EAP-FAST transaction. Cisco Secure ACS determines whether the PAC was generated using one of the master keys it is aware of, either active or retired (a PAC generated using a master key that has since expired can never be used to gain network access). When an end-user client has a PAC generated with an expired master key, the end-user client must receive a new PAC before EAP-FAST phase one can succeed. The means of providing PACs to end-user clients, known as PAC provisioning, are discussed in Automatic PAC Provisioning, page 10-18 and Manual PAC Provisioning, page 10-20.

After end-user clients are provided PACs, Cisco Secure ACS refreshes them as dictated by master key and PAC TTL values. Cisco Secure ACS generates and sends a new PAC as needed at the end of phase two of EAP-FAST; however, if you shorten the master key TTL, you may in effect be requiring PAC provisioning to occur. For more information about how master key and PAC states determine whether Cisco Secure ACS sends a new PAC to the end-user client at the end of phase two, see Master Key and PAC TTLs, page 10-21.

Regardless of the master key TTL values you define, a user will require PAC provisioning when the user does not use EAP-FAST to access the network before the master key used to generate the user's PAC has expired. For example, if the master key TTL is one week and the retired master key TTL is one week, each EAP-FAST end-user client used by someone who goes on vacation for two weeks will require PAC provisioning.



Downloaded from www.Manualslib.com manuals search engine

The following list contrasts the various means by which an end-user client can receive PACs:

- **PAC provisioning**—Required when an end-user client has no PAC or has a PAC that is based on an expired master key. For more information about how master key and PAC states determine whether PAC provisioning is required, see Master Key and PAC TTLs, page 10-21.

  Two means of PAC provisioning are supported:

  - **Automatic provision**—Sends a PAC using a secure network connection. For more information, see Automatic PAC Provisioning, page 10-18.
  - **Manual provision**—Requires that you use Cisco Secure ACS to generate a PAC file for the user, copy the PAC file to the computer running the end-user client, and import the PAC file into the end-user client. For more information, see Manual PAC Provisioning, page 10-20.

- **PAC refresh**—Occurs automatically when EAP-FAST phase two authentication has succeeded and master key and PAC TTLs dictate that the PAC must be refreshed. For more information about how master key and PAC states determine whether a PAC is refreshed, see Master Key and PAC TTLs, page 10-21.

PACs have the following two states, determined by the PAC TTL setting:

- **Active**—A PAC younger than the PAC TTL is considered active and can be used to complete EAP-FAST phase one, provided that the master key used to generate it has not expired. Regardless of whether a PAC is active, if it is based on an expired master key, PAC provisioning must occur before EAP-FAST phase one can succeed.
- **Expired**—A PAC older than the PAC TTL is considered expired. Provided that the master key used to generate the PAC has not expired, an expired PAC can be used to complete EAP-FAST phase one and, at the end of EAP-FAST phase two, Cisco Secure ACS will generate a new PAC for the user and provide it to the end-user client.

## Automatic PAC Provisioning

Automatic PAC provisioning sends a new PAC to an end-user client over a secured network connection. Automatic PAC provisioning requires no intervention of the network user or a Cisco Secure ACS administrator, provided that both Cisco Secure ACS and the end-user client are configured to support automatic provisioning.



Downloaded from www.Manualslib.com manuals search engine

EAP-FAST phase zero requires EAP-MSCHAPv2 authentication of the user. Upon successful user authentication, Cisco Secure ACS establishes a Diffie-Hellman tunnel with the end-user client. Cisco Secure ACS generates a PAC for the user and sends it to the end-user client within this tunnel, along with the Authority ID and Authority ID information about this Cisco Secure ACS.

**Note** Because EAP-FAST phase zero and phase two use different authentication methods (EAP-MSCHAPv2 in phase zero versus EAP-GTC in phase two), some databases that support phase two cannot support phase zero. Given that Cisco Secure ACS associates each user with a single user database, the use of automatic PAC provisioning requires that EAP-FAST users are authenticated with a database that is compatible with EAP-FAST phase zero. For the databases with which Cisco Secure ACS can support EAP-FAST phase zero and phase two, see Authentication Protocol-Database Compatibility, page 1-10.

No network service is enabled by phase zero of EAP-FAST; therefore, Cisco Secure ACS logs a EAP-FAST phase zero transaction in the Failed Attempts log, including an entry that PAC provisioning occurred. After the end-user client has received a PAC through a successful phase zero, it sends a new EAP-FAST request to begin phase one.

**Note** Because transmission of PACs in phase zero is secured by MS-CHAPv2 authentication and MS-CHAPv2 is vulnerable to dictionary attacks, we recommend that you limit use of automatic provisioning to initial deployment of EAP-FAST. After a large EAP-FAST deployment, PAC provisioning should be performed manually to ensure the highest security for PACs. For more information about manual PAC provisioning, see Manual PAC Provisioning, page 10-20.

To control whether Cisco Secure ACS performs automatic PAC provisioning, you use the options on the Global Authentication Setup page in the System Configuration section. For more information, see Authentication Configuration Options, page 10-27.



Downloaded from www.Manualslib.com manuals search engine

## Manual PAC Provisioning

Manual PAC provisioning requires a Cisco Secure ACS administrator to generate PAC files, which must then be distributed to the applicable network users. Users must configure end-user clients with their PAC files. For example, if your EAP-FAST end-user client is the Cisco Aironet Client Utility (ACU), configuring the ACU to support EAP-FAST requires that you import a PAC file. For more information about configuring a Cisco ACU, see the applicable configuration guide for your ACU.

You can use manual PAC provisioning to control who can use EAP-FAST to access your network. If you disable automatic PAC provisioning, any EAP-FAST user denied a PAC cannot access the network. If your Cisco Secure ACS deployment includes network segmentation wherein access to each network segment is controlled by a separate Cisco Secure ACS, manual PAC provisioning enables you to grant EAP-FAST access on a per-segment basis. For example, if your company uses EAP-FAST for wireless access in its Chicago and Boston offices and the Cisco Aironet Access Points at each of these two offices are configured to use different Cisco Secure ACSes, you can determine, on a per-employee basis, whether Boston employees visiting the Chicago office can have wireless access.

**Note** Replicating EAP-FAST master keys and policies affects the ability to require different PACs per Cisco Secure ACS. For more information, see Table 10-2.

While the administrative overhead of manual PAC provisioning is much greater than automatic PAC provisioning, it does not include the risk of sending the PAC over the network. When you first deploy EAP-FAST, using manual PAC provisioning would require a lot of manual configuration of end-user clients; however, it is the most secure means for distributing PACs. We recommend that, after a large EAP-FAST deployment, PAC provisioning should be performed manually to ensure the highest security for PACs.

You can generate PAC files for specific usernames, groups of users, lists of usernames, or all users. When you generate PAC files for groups of users or all users, the users must be known or discovered users and cannot be unknown users. Cisco Secure ACS for Windows Server supports the generation of PAC files with CSUtil.exe. For more information about generating PACs with CSUtil.exe, see PAC File Generation, page D-40.



Downloaded from www.Manualslib.com manuals search engine

## Master Key and PAC TTLs

The TTL values for master keys and PACs determine their states, as described in About Master Keys, page 10-15 and About PACs, page 10-17. Master key and PAC states determine whether someone requesting network access with EAP-FAST requires PAC provisioning or PAC refreshing. Table 10-1 summarizes Cisco Secure ACS behavior with respect to PAC and master key states.

*Table 10-1 Master Key versus PAC States*

| Master key state | PAC active | PAC expired |
|---|---|---|
| **Master key active** | Phase one succeeds.<br>PAC is *not* refreshed at end of phase two. | Phase one succeeds.<br>PAC is refreshed at end of phase two. |
| **Master key retired** | Phase one succeeds.<br>PAC is refreshed at end of phase two. | Phase one succeeds.<br>PAC is refreshed at end of phase two. |
| **Master key expired** | PAC provisioning is required.<br>If automatic provisioning is *enabled*, phase zero occurs and a new PAC is sent. The end-user client initiates a new EAP-FAST authentication request using the new PAC.<br>If automatic provisioning is *disabled*, phase zero does not occur and phase one fails. You must use manual provisioning to give the user a new PAC. | PAC provisioning is required.<br>If automatic provisioning is *enabled*, phase zero occurs and a new PAC is sent. The end-user client initiates a new EAP-FAST authentication request using the new PAC.<br>If automatic provisioning is *disabled*, phase zero does not occur and phase one fails. You must use manual provisioning to give the user a new PAC. |



Downloaded from www.Manualslib.com manuals search engine

## Replication and EAP-FAST

The CiscoSecure Database Replication feature supports the replication of EAP-FAST settings, Authority ID, and master keys. Replication of EAP-FAST data occurs only if the following are true:

- On the Database Replication Setup page of the primary Cisco Secure ACS, under Send, you have selected the EAP-FAST master keys and policies check box.
- On the Global Authentication Setup page of the primary Cisco Secure ACS, you have enabled EAP-FAST and selected the EAP-FAST master server check box.
- On the Database Replication Setup page of the secondary Cisco Secure ACS, under Receive, you have selected the **EAP-FAST master keys and policies** check box.
- On the Global Authentication Setup page of the secondary Cisco Secure ACS, you have enabled EAP-FAST and deselected the EAP-FAST master server check box.

EAP-FAST-related replication occurs for three events:

- **Generation of master keys**—A primary Cisco Secure ACS sends newly generated active and backup master keys to secondary Cisco Secure ACSes. This occurs immediately after master key generation, provided that replication is configured properly and is not affected by replication scheduling on the Database Replication Setup page.
- **Manual replication**—All EAP-FAST components that can be replicated are replicated if you click Replicate Now on the Database Replication Setup page of the primary Cisco Secure ACS. Some of the replicated components are configurable in the HTML interface. Whether an EAP-FAST component is replicated or configurable is detailed in Table 10-2.

  **Note** EAP-FAST replication is not included in scheduled replication events.

- **Changes to EAP-FAST settings**—If, on a primary Cisco Secure ACS, you change any EAP-FAST configurable components that are replicated, Cisco Secure ACS begins EAP-FAST replication. Whether an EAP-FAST component is replicated or configurable is detailed in Table 10-2.



Downloaded from www.Manualslib.com manuals search engine

The Database Replication log on the primary Cisco Secure ACS records replication of master keys. Entries related to master key replication contain the text "MKEYReplicate".

*Table 10-2 EAP-FAST Components and Replication*

| EAP-FAST Component | Replicated? | Configurable? |
|---|---|---|
| EAP-FAST Enable | No | Yes, on the Global Authentication Setup page. |
| Master key TTL | Yes | Yes, on the Global Authentication Setup page. |
| Retired master key TTL | Yes | Yes, on the Global Authentication Setup page. |
| PAC TTL | Yes | Yes, on the Global Authentication Setup page. |
| Authority ID | Yes | No, generated by Cisco Secure ACS. |
| Authority ID info | Yes | Yes, on the Global Authentication Setup page. |
| Client initial message | Yes | Yes, on the Global Authentication Setup page. |
| Master keys | Yes | No, generated by Cisco Secure ACS when TTL settings dictate. |
| EAP-FAST master server | No | Yes, on the Global Authentication Setup page. |
| Actual EAP-FAST server status | No | No, determined by Cisco Secure ACS. |

The EAP-FAST master server setting has a significant effect upon EAP-FAST authentication and replication, as follows:

- **Enabled**—When the EAP-FAST master server check box is selected, the "Actual EAP-FAST server status" is `Master` and Cisco Secure ACS ignores the EAP-FAST settings, Authority ID, and master keys it receives from a primary Cisco Secure ACS during replication, preferring instead to use master keys it generates, its unique Authority ID, and the EAP-FAST settings configured in its HTML interface.

  Enabling the EAP-FAST master server setting requires providing for the end-user client a PAC from the primary Cisco Secure ACS that is different than the PAC from the secondary Cisco Secure ACS. Because the primary and secondary Cisco Secure ACSes send different Authority IDs at the beginning of the EAP-FAST transaction, the end-user client must have a PAC for each Authority ID. A PAC generated by the primary Cisco Secure ACS is not



Downloaded from www.Manualslib.com manuals search engine

accepted by the secondary Cisco Secure ACS in a replication scheme where the EAP-FAST master server setting is enabled on the secondary Cisco Secure ACS.

**Tip** In a replicated Cisco Secure ACS environment, use the EAP-FAST master server feature in conjunction with disallowing automatic PAC provisioning to control EAP-FAST access to different segments of your network. Without automatic PAC provisioning, users must request PACs for each network segment.

- **Disabled**—When the EAP-FAST master server check box is not selected, Cisco Secure ACS continues to operate as an EAP-FAST master server until the first time it receives replicated EAP-FAST components from the primary Cisco Secure ACS. When "Actual EAP-FAST server status" displays the text `Slave`, Cisco Secure ACS uses the EAP-FAST settings, Authority ID, and master keys it receives from a primary Cisco Secure ACS during replication, rather than using master keys it generates and its unique Authority ID.

  **Note** When you deselect the EAP-FAST master server check box, the "Actual EAP-FAST server status" remains `Master` until Cisco Secure ACS receives replicated EAP-FAST components and then the "Actual EAP-FAST server status" changes to `Slave`. Until "Actual EAP-FAST server status" changes to `Slave`, Cisco Secure ACS acts as a master EAP-FAST server, using master keys it generates, its unique Authority ID, and the EAP-FAST settings configured in its HTML interface.

  Disabling the EAP-FAST master server setting eliminates the need for providing a different PAC from the primary and secondary Cisco Secure ACSes. This is because the primary and secondary Cisco Secure ACSes send the end-user client the same Authority ID at the beginning of the EAP-FAST transaction; therefore, the end-user client uses the same PAC in its response to either Cisco Secure ACS. Also, a PAC generated for a user by one Cisco Secure ACS in a replication scheme where the EAP-FAST master server setting is disabled is accepted by all other Cisco Secure ACSes in the same replication scheme.

For more information about replication, see CiscoSecure Database Replication, page 9-1.



Downloaded from www.Manualslib.com manuals search engine

# Enabling EAP-FAST

This procedure provides an overview of the detailed procedures required to configure Cisco Secure ACS to support EAP-FAST authentication.

**Note** End-user clients must be configured to support EAP-FAST. This procedure is specific to configuring Cisco Secure ACS only.

### Before You Begin

The steps in this procedure are a suggested order only. Enabling EAP-FAST at your site may require recursion of these steps or performing these steps in a different order. For example, in this procedure, determining how you want to support PAC provisioning comes after configuring a user database to support EAP-FAST; however, choosing automatic PAC provisioning places different limits upon user database support.

To enable Cisco Secure ACS to perform EAP-FAST authentication, follow these steps:

**Step 1** Configure a user database that supports EAP-FAST authentication. To determine which user databases support EAP-FAST authentication, see Authentication Protocol-Database Compatibility, page 1-10. For user database configuration, see Chapter 13, "User Databases".

**Note** User database support differs for EAP-FAST phase zero and phase two.

Cisco Secure ACS supports use of the Unknown User Policy and group mapping with EAP-FAST, as well as password aging with Windows external user databases.

**Step 2** Determine master key and PAC TTL values. While changing keys and PACs more frequently could be considered more secure, it also increases the likelihood that PAC provisioning will be needed for machines left offline so long that the PACs on them are based on expired master keys.

Also, if you reduce the TTL values that you initially deploy EAP-FAST with, you may force PAC provisioning to occur because users would be more likely to have PACs based on expired master keys.



Downloaded from www.Manualslib.com manuals search engine

For information about how master key and PAC TTL values determine whether PAC provisioning or PAC refreshing is required, see Master Key and PAC TTLs, page 10-21.

**Step 3** Determine whether you want to use automatic or manual PAC provisioning. For more information about the two means of PAC provisioning, see Automatic PAC Provisioning, page 10-18, and Manual PAC Provisioning, page 10-20.

**Note** We recommend limiting the use of automatic PAC provisioning to initial deployments of EAP-FAST, followed by using manual PAC provisioning for adding small numbers of new end-user clients to your network and for replacing PACs based on expired master keys.

**Step 4** Using the decisions during Step 2 and Step 3, enable EAP-FAST on the Global Authentication Setup page. For detailed steps, see Configuring Authentication Options, page 10-33.

Cisco Secure ACS is ready to perform EAP-FAST authentication.

# Global Authentication Setup

The Global Authentication Setup page provides a means to enable or disable some of the authentication protocols supported by Cisco Secure ACS. You can also configure other options for some of the protocols represented on the Global Authentication Setup page.

This section contains the following topics:

- Authentication Configuration Options, page 10-27
- Configuring Authentication Options, page 10-33



Downloaded from www.Manualslib.com manuals search engine

# Authentication Configuration Options

The Global Authentication Setup page contains the following configuration options:

- **PEAP**—You can configure the following options for PEAP:
  - **Allow EAP-MSCHAPv2**—Whether Cisco Secure ACS attempts EAP-MSCHAPv2 authentication with PEAP clients.

**Note** If both the Allow EAP-MSCHAPv2 and the Allow EAP-MSCHAPv2 check boxes are selected, Cisco Secure ACS negotiates the EAP type with the end-user PEAP client.

  - **Allow EAP-GTC**—Whether Cisco Secure ACS attempts EAP-GTC authentication with PEAP clients.
  - **Cisco client initial message**—The message you want displayed during PEAP authentication. The PEAP client initial display message is the first challenge a user of a Cisco Aironet PEAP client sees when attempting authentication. It should direct the user on what to do next, for example, "Enter your passcode." The message is limited to 60 characters.
  - **PEAP session timeout (minutes)**—The maximum PEAP session length you want to allow users, in minutes. A session timeout value greater than 0 (zero) enables the PEAP session resume feature, which caches the TLS session created in phase one of PEAP authentication. When a PEAP client reconnects, Cisco Secure ACS uses the cached TLS session to restore the session, which improves PEAP performance. Cisco Secure ACS deletes cached TLS sessions when they time out. The default timeout value is 120 minutes. To disable the session resume feature, set the timeout value to 0 (zero).
  - **Enable Fast Reconnect**—Whether Cisco Secure ACS resumes sessions for PEAP clients without performing phase two of PEAP authentication. Deselecting the Enable Fast Reconnect check box causes Cisco Secure ACS to always perform phase two of PEAP authentication, even when the PEAP session has not timed out.

    Fast reconnection can occur only when Cisco Secure ACS allows the session to resume because the session has not timed out. If you disable the PEAP session resume feature by entering 0 (zero) in the PEAP



Downloaded from www.Manualslib.com manuals search engine

session timeout (minutes) box, selecting the Enable Fast Reconnect check box has no effect on PEAP authentication and phase two of PEAP authentication always occurs.

- **EAP-FAST**—You can configure the following options for EAP-FAST:
  - **Allow EAP-FAST**—Whether Cisco Secure ACS permits EAP-FAST authentication.

**Note** If users access your network using a AAA client defined in the Network Configuration section as a RADIUS (Cisco Aironet) device, one or more of the LEAP, EAP-TLS, or EAP-FAST protocols must be enabled on the Global Authentication Setup page; otherwise, Cisco Aironet users cannot authenticate.

  - **Master Key TTL**—The duration that a master key is used to generate new PACs. When the master key becomes older than the master key TTL, Cisco Secure ACS retires the master key and generates a new master key. The default master key TTL is one month.

**Note** Decreasing the master key TTL can cause retired master keys to expire because a master key expires when it is older than the sum of the master key TTL and the retired master key TTL; therefore, decreasing the master key TTL requires PAC provisioning for end-user clients with PACs based on the newly expired master keys.

For more information about master keys, see About Master Keys, page 10-15.

  - **Retired master key TTL**—The duration that PACs generated using a retired master key are acceptable for EAP-FAST authentication. In other words, the retired master key TTL defines the length of the grace period during which PACs generated with a master key that is no longer active are acceptable. When an end-user client gains network access using a PAC based on a retired master key, Cisco Secure ACS sends a new PAC to the end-user client. The default retired master key TTL is three months.

    When a retired master key ages past the retired master key TTL, it expires and Cisco Secure ACS deletes it.



Downloaded from www.Manualslib.com manuals search engine

**Note** Decreasing the retired master key TTL is likely to cause some retired master keys to expire; therefore, end-user clients with PACs based on the newly expired master keys require PAC provisioning.

**Note** Decreasing the retired master key TTL can cause retired master keys to expire; therefore, decreasing the retired master key TTL requires PAC provisioning for end-user clients with PACs based on the newly expired master keys.

For more information about master keys, see About Master Keys, page 10-15.

- **PAC TTL**—The duration that a PAC is used before it expires and must be replaced. If the master key used to generate it has not expired, new PAC creation and assignment are automatic. If the master key used to generate it has expired, in-band or out-of-band provisioning must be used to provide the end-user client with a new PAC. The default PAC TTL is one week.

  For more information about PACs, see About PACs, page 10-17.

- **Client initial display message**—Specifies a message to be sent to users who authenticate with an EAP-FAST client. Maximum length is 40 characters.

**Note** A user will see the initial display message only if the end-user client supports its display.

- **Authority ID Info**—A short description of this Cisco Secure ACS, sent along with PACs issued by Cisco Secure ACS. EAP-FAST end-user clients use it to describe the AAA server that issued the PAC. Maximum length is 64 characters.



Downloaded from www.Manualslib.com manuals search engine

**Note** Authority ID information is not the same as the Authority ID, which is generated automatically by Cisco Secure ACS and is not configurable. While the Authority ID is used by end-user clients to determine which PAC to send to Cisco Secure ACS, the Authority ID information is strictly the human-readable label associated with the Authority ID.

- **Allow automatic PAC provisioning**—Whether Cisco Secure ACS will provision an end-user client with a PAC using EAP-FAST phase 0. If this check box is selected, Cisco Secure ACS establishes a secured connection with the end-user client for providing a new PAC. If the check box is not selected, Cisco Secure ACS denies the user access and PAC provisioning must be performed out of band (manually).
- **EAP-FAST Master Server**—When this check box is not selected and when Cisco Secure ACS receives replicated EAP-FAST policies, Authority ID, and master keys, Cisco Secure ACS uses them rather than its own EAP-FAST policies, Authority ID, and master keys.

  When this check box is selected, Cisco Secure ACS uses its own EAP-FAST policies, Authority ID, and master keys. For more information, see Table 10-2.

**Note** Click Submit + Restart if you change the EAP-FAST master server setting.

- **Actual EAP-FAST server status**—This read-only option displays the state of Cisco Secure ACS with respect to EAP-FAST. If this option displays “Master”, Cisco Secure ACS generates its own master keys and Authority ID. If this option displays “Slave”, Cisco Secure ACS uses master keys and the Authority ID it receives during replication. For more information, see Table 10-2.

**Tip** If you deselect the EAP-FAST Master Server check box, EAP-FAST server status remains “Master” until Cisco Secure ACS receives replicated EAP-FAST components.



Downloaded from www.Manualslib.com manuals search engine

- **EAP-TLS**—You can configure the following options for EAP-TLS:
  - **Allow EAP-TLS**—Whether Cisco Secure ACS permits EAP-TLS authentication.

**Note** If users access your network using a AAA client defined in the Network Configuration section as a RADIUS (Cisco Aironet) device, one or more of the LEAP, EAP-TLS, or EAP-FAST protocols must be enabled on the Global Authentication Setup page; otherwise, Cisco Aironet users cannot authenticate.

  - **Certificate SAN comparison**—Whether authentication is performed by comparing the Subject Alternative Name (SAN) of the end-user client certificate to the username in the applicable user database.

**Note** If you select more than one comparison type, Cisco Secure ACS performs the comparisons in the order listed. If the one comparison type fails, Cisco Secure ACS attempts the next enabled comparison type. Comparison stops after the first successful comparison.

  - **Certificate CN comparison**—Whether authentication is performed by comparing the Common Name of the end-user client certificate to the username in the applicable user database.
  - **Certificate Binary comparison**—Whether authentication is performed by a binary comparison of the end-user client certificate to the user certificate stored in the applicable user database. This comparison method cannot be used to authenticate users stored in an ODBC external user database.
  - **EAP-TLS session timeout (minutes)**—The maximum EAP-TLS session length you want to allow users, in minutes. A session timeout value greater than 0 (zero) enables the EAP-TLS session resume feature. The session resume feature allows users to reauthenticate without a user lookup or certificate comparison provided that the session has not timed out. If the end-user client is restarted, authentication requires a certificate lookup even if the session timeout interval has not ended. The default timeout value is 120 minutes. To disable the session timeout feature, set the timeout value to 0 (zero).



Downloaded from www.Manualslib.com manuals search engine

- **LEAP**—The Allow LEAP (For Aironet only) check box controls whether Cisco Secure ACS performs LEAP authentication. LEAP is currently used only for Cisco Aironet wireless networking. If you disable this option, Cisco Aironet end-user clients configured to perform LEAP authentication cannot access the network. If all Cisco Aironet end-user clients use a different authentication protocol, such as EAP-TLS, we recommend that you disable this option.

  **Note** If users access your network using a AAA client defined in the Network Configuration section as a RADIUS (Cisco Aironet) device, either LEAP, EAP-TLS, or both must be enabled on the Global Authentication Setup page; otherwise, Cisco Aironet users cannot authenticate.

- **EAP-MD5**—The Allow EAP-MD5 check box controls whether Cisco Secure ACS performs EAP-MD5 authentication. If you disable this option, end-user clients configured to perform EAP-MD5 authentication cannot access the network. If no end-user clients use EAP-MD5, we recommend that you disable this option.
- **AP EAP request timeout (seconds)**—Whether Cisco Secure ACS instructs Cisco Aironet Access Points (APs) to use the specified timeout value during EAP conversations. The value specified must be the number of seconds after which Cisco Aironet APs should assume that an EAP transaction with Cisco Secure ACS has been lost and should be restarted. A value of 0 (zero) disables this feature.

  During EAP conversations, Cisco Secure ACS sends the value defined in the AP EAP request timeout box using the IETF RADIUS Session-Timeout (27) attribute; however, in the RADIUS Access-Accept packet at the end of the conversation, the value that Cisco Secure ACS sends in the IETF RADIUS Session-Timeout (27) attribute is the value specified in the Cisco Aironet RADIUS VSA Cisco-Aironet-Session-Timeout (01) or, if that attribute is not enabled, the IETF RADIUS Session-Timeout (27) attribute.



Downloaded from www.Manualslib.com manuals search engine

**Note** Cisco Aironet RADIUS VSA Cisco-Aironet-Session-Timeout (01) is not a true RADIUS VSA; instead, it represents the value that Cisco Secure ACS sends in the IETF RADIUS Session-Timeout attribute when the AAA client sending the RADIUS request is defined in the Network Configuration as authenticating with RADIUS (Cisco Aironet).

- **MS-CHAP Configuration**—The Allow MS-CHAP Version 1 Authentication and Allow MS-CHAP Version 2 Authentication check boxes control whether Cisco Secure ACS performs MS-CHAP authentication for RADIUS requests. The two check boxes allow you to further control which versions of MS-CHAP are permitted in RADIUS requests. If you disable a particular version of MS-CHAP, end-user clients configured to authenticate with that version using RADIUS cannot access the network. If no end-user clients are configured to use a specific version of MS-CHAP with RADIUS, we recommend that you disable that version of MS-CHAP.

**Note** For TACACS+, Cisco Secure ACS supports only MS-CHAP version 1. TACACS+ support for MS-CHAP version 1 is always enabled and is not configurable.

# Configuring Authentication Options

Use this procedure to select and configure how Cisco Secure ACS handles options for authentication. In particular, use this procedure to specify and configure the varieties of EAP that you allow, and to specify whether you allow either MS-CHAP Version 1 or MS-CHAP Version 2, or both.

For more information on the EAP-TLS Protocol, see EAP-TLS Authentication, page 10-2. For more information on the PEAP protocol, see PEAP Authentication, page 10-8. For more information on the PEAP protocol, see EAP-FAST Authentication, page 10-13. For details regarding how various password protocols are supported by the various databases, see Authentication Protocol-Database Compatibility, page 1-10.



Downloaded from www.Manualslib.com manuals search engine

### Before You Begin

For information about the options on the Global Authentication Setup page, see Authentication Configuration Options, page 10-27.

To configure authentication options, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Global Authentication Setup**.

Cisco Secure ACS displays the Global Authentication Setup page.

**Step 3** Configure options, as applicable. For more information about the significance of the options, see Authentication Configuration Options, page 10-27.

**Step 4** If you want to immediately implement the settings you have made, click **Submit + Restart**.

Cisco Secure ACS restarts its services and implements the authentication configuration options you selected.

**Step 5** If you want to save the settings you have made but implement them later, click **Submit**.

**Tip** You can restart Cisco Secure ACS services at any time by using the Service Control page in the System Configuration section.

Cisco Secure ACS saves the authentication configuration options you selected.

# Cisco Secure ACS Certificate Setup

This section contains the following topics:


- Installing a Cisco Secure ACS Server Certificate, page 10-35
- Adding a Certificate Authority Certificate, page 10-37
- Editing the Certificate Trust List, page 10-38
- Managing Certificate Revocation Lists, page 10-40
- Generating a Certificate Signing Request, page 10-45




Downloaded from www.Manualslib.com manuals search engine

- Using Self-Signed Certificates, page 10-47
- Updating or Replacing a Cisco Secure ACS Certificate, page 10-50

# Installing a Cisco Secure ACS Server Certificate

Perform this procedure to install (that is, enroll) a server certificate for your Cisco Secure ACS. You can perform certificate enrollment to support EAP-TLS and PEAP authentication, as well as to support HTTPS protocol for GUI access to Cisco Secure ACS. There are three basic options for how you obtain your server certificate; you may:

- Obtain a certificate from a CA
- Use an existing certificate from local machine storage
- Generate a self-signed certificate.

**Before You Begin**

You must have a server certificate for your Cisco Secure ACS before you can install it. With Cisco Secure ACS, certificate files must be in Base64-encoded X.509. If you do not already have a server certificate in storage, you can use the procedure in Generating a Certificate Signing Request, page 10-45, or any other means, to obtain a certificate for installation.

If you are installing a server certificate that replaces an existing server certificate, the installation could affect the configuration of the CTL and CRL settings your Cisco Secure ACS. After you have installed a replacement certificate, you should determine whether you need to reconfigure any CTL or CRL settings.

If you want to use a server certificate from local machine storage, we recommend that you read *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks*, available on the Cisco Secure ACS CD and at http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml. This white paper provides information about how to add a certificate to machine storage and how to configure a Microsoft certification authority server for use with Cisco Secure ACS.

To install an existing certificate for use on Cisco Secure ACS, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Certificate Setup**.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** Click **Install ACS Certificate**.

Cisco Secure ACS displays the Install ACS Certificate page.

**Step 4** You must specify whether Cisco Secure ACS reads the certificate from a specified file or uses a certificate already in storage on the local machine. Do one of the following:

- To specify that Cisco Secure ACS reads the certificate from a specified file, select the **Read certificate from file** option, and then type the full directory path and filename of the certificate file in the Certificate file box.
- To specify that Cisco Secure ACS uses a particular existing certificate from local machine certificate storage, select the **Use certificate from storage** option, and then type the certificate CN (common name/subject name) in the Certificate CN box.

**Tip** Type the certificate CN only; omit the **cn=** prefix.

**Step 5** If you generated the request using Cisco Secure ACS, in the Private key file box, type the full directory path and name of the file that contains the private key.

**Note** If the certificate was installed in storage with the private key, you do not have the private key file and do not need to type it.

**Tip** This is the private key associated with the server certificate.

**Step 6** In the Private key password box, type the private key password.

**Tip** If you used Cisco Secure ACS to generate the certificate signing request, this is the value you entered in *Private key password* on the Generate Certificate Signing Request page. If the private key file is unencrypted, leave this box empty.



Downloaded from www.Manualslib.com manuals search engine

**Step 7** Click **Submit**.

To show that the certificate setup is complete, Cisco Secure ACS displays the Installed Certificate Information table, which contains the following certificate information:

- Issued to: *certificate subject*
- Issued by: *CA common name*
- Valid from:
- Valid to:
- Validity

# Adding a Certificate Authority Certificate

Use this procedure to add new certification authority (CA) certificates to Cisco Secure ACS local certificate storage.

**Note** If the clients and Cisco Secure ACS are getting their certificates from the same CA, you do not need to perform this procedure because Cisco Secure ACS automatically trusts the CA that issued its certificate.

When a user certificate is from an unknown CA (that is, one that is different from the CA that certifies the Cisco Secure ACS), you must specifically configure Cisco Secure ACS to trust that CA or authentication fails. Until you perform this procedure to explicitly extend trust by adding another CA, Cisco Secure ACS only recognizes certificates from the CA that issued its own certificate.

Configuring Cisco Secure ACS to trust a specific CA is a two-step process that comprises both this procedure of adding a CA's certificate and the procedure in Editing the Certificate Trust List, page 10-38, where you signify that the particular CA is to be trusted. (Cisco Secure ACS comes configured with a list of popular CAs, none of which are enabled until you explicitly signify trustworthiness.)



Downloaded from www.Manualslib.com manuals search engine

To add a certificate authority certificate to your local storage, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Certificate Setup**.

**Step 3** Click **ACS Certification Authority Setup**.

Cisco Secure ACS displays the CA Operations table on the Certification Authorities Setup page.

**Step 4** In the CA certificate file box, type the full path and filename for the certificate you want to use.

**Step 5** Click **Submit**.

The new CA certificate is added to local certificate storage. And, if it is not already there, the name of the CA that issued the certificate is placed on the CTL.

**Tip** To use this new CA certificate to authenticate users, you must edit the certificate trust list to signify that this CA is trusted. For more information, see Editing the Certificate Trust List, page 10-38.

# Editing the Certificate Trust List

Cisco Secure ACS uses the CTL to verify the client certificates. For a CA to be trusted by Cisco Secure ACS, its certificate must be installed, and the Cisco Secure ACS administrator must explicitly configure the CA as trusted by editing the CTL. If the Cisco Secure ACS server certificate is replaced, the CTL is erased; you must configure the CTL explicitly each time you install or replace a Cisco Secure ACS server certificate.

**Note** The single exception to the requirement that a CA must be explicitly signified as trustworthy occurs when the clients and Cisco Secure ACS are getting their certificates from the same CA. You do not need to add this CA to the CTL because Cisco Secure ACS automatically trusts the CA that issued its certificate.



Downloaded from www.Manualslib.com manuals search engine

How you edit your CTL determines the type of trust model you have. Many use a restricted trust model wherein very few, privately controlled CAs are trusted. This model provides the highest level of security but restricts adaptability and scalability. The alternative, an open trust model, allows for more CAs or public CAs. This open trust model trades increased security for greater adaptability and scalability.

We recommend that you fully understand the implications of your trust model before editing the CTL in Cisco Secure ACS.

Use this procedure to configure CAs on your CTL as trusted or not trusted. Before a CA can be configured as trusted on the CTL, you must have added the CA to the local certificate storage; for more information, see Adding a Certificate Authority Certificate, page 10-37. If a user's certificate is from a CA that you have not specifically configured Cisco Secure ACS to trust, authentication fails.

To edit the CTL, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Cisco Secure ACS Certificate Setup**.

**Step 3** Click **Edit Certificate Trust List**.

The Edit the Certificate Trust List (CTL) table appears.

**Warning** **Adding a public CA, which you do not control, to your CTL, may reduce your system security.**

**Step 4** To configure a CA on your CTL as trusted, select the corresponding check box.

**Tip** You can select, or deselect, as many CAs as you want. Deselecting a CA's check box configures the CA as not trusted.

**Step 5** Click **Submit**.

Cisco Secure ACS configures the specified CA (or CAs) as trusted or not trusted in accordance with selecting or deselecting check boxes.



Downloaded from www.Manualslib.com manuals search engine

# Managing Certificate Revocation Lists

Certificate revocation lists (CRLs) are the means by which Cisco Secure ACS determines that the certificates employed by users seeking authentication are still valid, according to the CA that issued them.

This section contains the following topics:


- About Certificate Revocation Lists, page 10-40
- Certificate Revocation List Configuration Options, page 10-41
- Adding a Certificate Revocation List Issuer, page 10-42
- Editing a Certificate Revocation List Issuer, page 10-44
- Deleting a Certificate Revocation List Issuer, page 10-44


## About Certificate Revocation Lists

When a digital certificate is issued, you generally expect it to remain valid throughout its predetermined period of validity. However, various circumstances may call for invalidating the certificate earlier than expected. Such circumstances might include compromise or suspected compromise of the corresponding private key, or a change in the CAs issuance program. Under such circumstances, a CRL provides the mechanism by which the CA revokes the legitimacy of a certificate and calls for its managed replacement.

Cisco Secure ACS performs certificate revocation using the X.509 CRL profile. A CRL is a signed and time-stamped data structure issued by a CA (or CRL issuer) and made freely available in a public repository (for example, in an LDAP server). Details on the operation of the X.509 CRL profile are contained in RFC3280.

CRL functionality in Cisco Secure ACS includes the following:

- **Trusted publishers and repositories configuration**—In the Cisco Secure ACS HTML interface, you can view and configure CRL issuers and their CRL Distribution Points (CDPs) and periods.
- **Retrieval of CRLs from a CDP**—Using a transport protocol (LDAP or HTPP), Cisco Secure ACS is configured to periodically retrieve CRLs for each CA you configure. These CRLs are stored for use during EAP-TLS authentication. Note that there is no timestamp mechanism; Cisco Secure ACS waits for a specified period of time and then automatically downloads



Downloaded from www.Manualslib.com manuals search engine

the CRL. If the new CRL differs from the existing CRL, the new version is saved and added to the local cache. CRL retrievals appear in the log for the CSAuth service only when you have configured the level of detail in service logs to "full". The status, date, and time of the last retrieval is shown on the Certificate Revocation List Issuer edit page of the Cisco Secure ACS HTML interface.

**Note** Automatic CRL retrieval scheduling only functions if EAP-TLS is enabled.

- **Verification of certificate status**—During EAP-TLS authentication, Cisco Secure ACS checks the certificate presented by the user against the corresponding CRL issued by the CA of the user's certificate. If, according to the CRL currently stored by Cisco Secure ACS, the certificate has been revoked, authentication fails.

CRL issuers can only be added in association with trusted CAs (that is, CAs on the CTL). If you install a new server certificate for Cisco Secure ACS, your CTL is cleared of all trust relationships. While you must reestablish CAs on the CTL, the associated CRLs that you previously configured remain in place and do not have to be reconfigured.

## Certificate Revocation List Configuration Options

The Certificate Revocation List Issuers edit page contains the following configuration options:

- **Name**—A name you give this CRL issuer.
- **Description**—A description you give this CRL issuer.
- **Issuer's Certificate**—The CA certificate to be used when verifying the issuer's signature over the CRL data. This list is derived from the contents of your configured CTL.
- **CRL Distribution URL**—The URL you enter that specifies the URL that Cisco Secure ACS should use to retrieve the CRL. You can specify a URL that uses HTTP or LDAP. Be sure you specify a URL for the CRL corresponding to the CA you selected from the Issuer's Certificate list. Alternatively, you could specify the URL for the file itself; but this is only necessary in the case where the repository URL lists multiple files.



Downloaded from www.Manualslib.com manuals search engine

- **Retrieve CRL every**—The quantity and period of time that Cisco Secure ACS should wait between retrieving a CRL. For example 10 Days or 2 Months.
- **Retrieve on "Submit"**—Selecting this option causes Cisco Secure ACS to immediately attempt to contact the distribution URL and obtain the current CRL when the new CRL request page is submitted for processing. We recommend that you select this option when first obtaining a CRL to ensure that the CRL is obtained successfully.

The Certificate Revocation List Issuers edit page also contains a line, at the bottom of the table, titled Last Retrieve date:. This entry lists the status and the date and time of the last CRL retrieval or retrieval attempt.

## Adding a Certificate Revocation List Issuer

### Before You Begin

Before adding a CRL issuer to Cisco Secure ACS, you should ensure that you have listed the corresponding CA on the system's CTL, and you have determined the URL of the CRL distribution repository for the appropriate issuer and class of certificate. For the automatic CRL retrieval function to operate, ensure that you have enabled EAP-TLS.

To add a certificate revocation list issuer to Cisco Secure ACS, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Certificate Setup**.

**Step 3** Click **Certificate Revocation Lists**.

Cisco Secure ACS displays the CRL Issuers edit page.

**Step 4** Click **Add**.

**Step 5** In the Name box, type a name for this CRL issuer.

**Step 6** In the Description box, type a description for this CRL issuer.

**Step 7** In the Issuer's Certificate box, use the drop-down arrow to select from the list the CA certificate associated with this CRL issuer.



Downloaded from www.Manualslib.com manuals search engine

**Tip** Only CRL Issuers that are listed on the CTL are listed as possible selections. That is, you must list an entity as trusted on the CTL before you can select their Issuer's Certificate.

**Step 8** In the CRL Distribution URL box, type the URL for CRL distribution repository.

**Tip** The URL must specify the CRL itself when the repository contains multiple files.

**Step 9** In the Retrieve CRL every box, type the quantity and period of time that Cisco Secure ACS should wait between retrieving a CRL.

**Step 10** Select the **Retrieve on "Submit"** option to have Cisco Secure ACS attempt to obtain the current CRL when the page is submitted for processing.

**Tip** Selecting the Retrieve on "Submit" option is recommended. If Cisco Secure ACS cannot obtain the CRL from the distribution repository you listed, it displays the following error message: `Failed to retrieve CRL. Verify the CRL Distribution URL.`

**Step 11** Click **Submit**.

The specified CRL is added to Cisco Secure ACS (or is scheduled to be added if the Retrieve on "Submit" option was not selected).

**Tip** You can refer to the Last Retrieve date: box to see the status, date, and time of the last retrieval attempt.



Downloaded from www.Manualslib.com manuals search engine

## Editing a Certificate Revocation List Issuer

To edit a certificate revocation list issuer, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Certificate Setup**.

**Step 3** Click **Certificate Revocation Lists**.

Cisco Secure ACS displays the CRL Issuers edit page.

**Step 4** Click the name of the CRL issuer you want to edit.

The system displays the details of the CRL issuer that you chose.

**Step 5** Edit the information and settings you want to change.

**Step 6** Click **Submit**.

The corresponding CRL is changed in Cisco Secure ACS to that of the edited issuer (or is scheduled to be changed if the Retrieve on "Submit" option was not selected).

**Tip** You can refer to the **Last Retrieve date:** box to see the status, date, and time of the last CRL retrieval attempt.

## Deleting a Certificate Revocation List Issuer

To delete a certificate revocation list issuer, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Certificate Setup**.

**Step 3** Click **Certificate Revocation Lists**.

Cisco Secure ACS displays the CRL Issuers edit page.

**Step 4** Click the name of the CRL issuer you want to delete.

The system displays the details of the CRL issuer that you selected.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** Click **Delete**.

The specified CRL issuer, and all CRLs from that issuer, is deleted from Cisco Secure ACS.

# Generating a Certificate Signing Request

You can use Cisco Secure ACS to generate a certificate signing request (CSR). After you generate a CSR, you can submit it to a CA to obtain your certificate. You perform this procedure to generate the CSR for future use with a certificate enrollment tool.

**Note** If you already have a server certificate, you do not need to use this portion of the ACS Certificate Setup page.

To generate a certificate signing request, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Certificate Setup** and then click **Generate Certificate Signing Request**.

Cisco Secure ACS displays the Generate Certificate Signing Request page.

**Step 3** In the Certificate subject box, type values for the certificate fields required by the CA you want to submit the CSR to. A CN field is mandatory. The format is:

*field*=*value*, *field*=*value*, . . .

where *field* is the field name, such as CN, and *value* is the applicable value for the field, such as acs01primary. You can type a maximum of 256 characters in the "Certificate subject" box. Separate multiple values with commas. For example:

```
CN=acs01primary, O=WestCoast, C=US, S=California
```

The following table defines the valid fields that you can include in the "Certificate subject" box.



Downloaded from www.Manualslib.com manuals search engine

| Field | Field Name | Min. Length | Max. Length | Required? |
|---|---|---|---|---|
| CN | commonName | 1 | 64 | Yes |
| OU | organizationalUnitName | — | — | No |
| O | organizationName | — | — | No |
| S | stateOrProvinceName | — | — | No |
| C | countryName | 2 | 2 | No |
| E | emailAddress | 0 | 40 | No |
| L | localityName | — | — | No |

**Step 4** In the Private key file box, type the full directory path and name of the file in which the private key is saved, for example, `c:\privateKeyFile.pem`.

**Step 5** In the Private key password box, type the private key password (that you have invented).

**Step 6** In the Retype private key password box, retype the private key password.

**Step 7** From the Key length list, select the length of the key to be used.

**Tip** The choices for Key length are 512 or 1024 bits. The default and more secure choice is 1024 bits.

**Step 8** From the Digest to sign with list, select the digest (or hashing algorithm). The choices for are MD2, MD5, SHA, and SHA1. The default is SHA1.

**Step 9** Click **Submit**.

Cisco Secure ACS displays a CSR on the right side of the browser.

**Step 10** Submit the CSR to the CA of your choice.

After you receive the certificate from the CA, you can perform the steps in Installing a Cisco Secure ACS Server Certificate, page 10-35.



Downloaded from www.Manualslib.com manuals search engine

# Using Self-Signed Certificates

You can use Cisco Secure ACS to generate a self-signed digital certificate to be used for PEAP authentication protocol or for HTTPS support of Cisco Secure ACS administration. This capability supports TLS/SSL protocols and technologies without the requirement of interacting with a CA.

This section contains the following topics:


- About Self-Signed Certificates, page 10-47
- Self-Signed Certificate Configuration Options, page 10-48
- Generating a Self-Signed Certificate, page 10-49


## About Self-Signed Certificates

Cisco Secure ACS supports TLS/SSL-related protocols, including PEAP and HTTPS, that require the use of digital certificates. Employing self-signed certificates is a way for administrators to meet this requirement without having to interact with a certification authority (CA) to obtain and install the certificate for the Cisco Secure ACS. The self-signed certificate feature in Cisco Secure ACS allows the administrator to generate the self-signed digital certificate and use it for PEAP authentication protocol or for HTTPS support in web administration service.

Other than the lack of interaction with a CA to obtain the certificate, installing a self-signed certificate requires exactly the same actions as any other digital certificate. Although Cisco Secure ACS does not support the replication of self-signed certificates, you can export a certificate for use on more than one Cisco Secure ACS. To do this, you copy the certificate file (.cer format) and the corresponding private key file (.pvk format) to another Cisco Secure ACS where you then install the certificate in the standard manner. For information on installing certificates, see Installing a Cisco Secure ACS Server Certificate, page 10-35.

To ensure that a self-signed certificate interoperates with the client, refer to your client documentation. You may find that you must import the self-signed server certificate as a CA certificate on your particular client.



Downloaded from www.Manualslib.com manuals search engine

## Self-Signed Certificate Configuration Options

The Generate Self-Signed Certificate edit page contains the following mandatory configuration fields:

- **Certificate subject**—The subject for the certificate, prefixed with "cn=". We recommend using the Cisco Secure ACS name. For example, "cn=ACS11". The Certificate subject field here can contain a number of content entries as comma-separated items; these include:
  - **CN**—common name (the mandatory entry)
  - **OU**—organizational unit name
  - **O**—organization name
  - **S**—state or province
  - **E**—email address
  - **L**—locality name

  For example, the Certificate subject field might appear as follows:

  ```
  cn=ACS 11, O=Acme Enterprises, E=admin@acme.com
  ```

- **Certificate file**—The full path and filename for the certificate file that you want to generate. For example, "c:\acs_server_cert\acs_server_cert.cer". When you submit this page, Cisco Secure ACS creates the certificate file using the location and filename you specify.
- **Private key file**—The full path and filename for the private key file you want to generate. For example, "c:\acs_server_cert\acs_server_cert.pvk". When you submit this page, Cisco Secure ACS creates the private key file using the location and filename you specify.
- **Private key password**—A private key password for the certificate. Minimum length for the private key password is 4 characters, and the maximum length is 64 characters.
- **Retype private key password**—The private key password typed again, to ensure accuracy.
- **Key length**—Select the key length from the choices listed. The choices include 512 bits, 1024 bits, and 2048 bits.



Downloaded from www.Manualslib.com manuals search engine

- **Digest to sign with**—Select the hash digest to be used to encrypt the key from the choices listed. The choices include SHA1, SHA, MD2, and MD5.
- **Install generated certificate**—Select this check box if you want Cisco Secure ACS to install the self-signed certificate that it generates when you click Submit. If you employ this option, Cisco Secure ACS services must be restarted after you submit the page for the new settings to be adopted. If you do not select this option, the certificate file and private key file are generated and saved, but are not installed into local machine storage.

## Generating a Self-Signed Certificate

All fields on the Generate Self-Signed Certificate page are mandatory. For information on the fields' contents, see Self-Signed Certificate Configuration Options, page 10-48.

To generate a self-signed certificate, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Certificate Setup**.

**Step 3** Click **Generate Self-Signed Certificate**.

Cisco Secure ACS displays the Generate Self-Signed Certificate edit page.

**Step 4** In the Certificate subject box, type the certificate subject in the form *cn=XXXX*. You can enter additional information here, for information see Self-Signed Certificate Configuration Options, page 10-48.

**Step 5** In the Certificate file box, type the full path and file name for the certificate file.

**Step 6** In the Private key file box, type the full path and file name for the private key file.

**Step 7** In the Private key password box, type the private key password.

**Step 8** In the Retype private key password box, retype the private key password.

**Step 9** In the Key length box, select the key length.

**Step 10** In the Digest to sign with box, select the hash digest to be used to encrypt the key.



Downloaded from www.Manualslib.com manuals search engine

**Step 11** To install the self-signed certificate when you submit the page, select the **Install generated certificate** option.

**Note** If you use the Install generated certificate option you must restart Cisco Secure ACS services after submitting this form to adopt the new settings.

**Tip** If you do not select the Install generated certificate option, the certificate file and private key file are generated and saved when you click Submit in the next step, but are not installed into local machine storage.

**Step 12** Click **Submit**.

The specified certificate and private key files are generated and stored, as specified. The certificate becomes operational, if you also selected the Install generated certificate option, only after you restart Cisco Secure ACS services.

# Updating or Replacing a Cisco Secure ACS Certificate

Use this procedure to update or replace an existing Cisco Secure ACS certificate that is out-of-date or out-of-order.

**Caution** This procedure eliminates your existing Cisco Secure ACS certificate and erases your CTL configuration.

To install a new ACS certificate, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **ACS Certificate Setup**.

Cisco Secure ACS displays the Installed Certificate Information table on the ACS Certificate Setup page.



Downloaded from www.Manualslib.com manuals search engine

**Note** If your Cisco Secure ACS has not already been enrolled with a certificate, you do not see the Installed Certificate Information table. Rather, you see the Install new certificate table. If this is the case, you can proceed to Step 5.

**Step 3** Click **Enroll New Certificate**.

A confirmation dialog box appears.

**Step 4** To confirm that you intend to enroll a new certificate, click **OK**.

The existing Cisco Secure ACS certificate is removed and your CTL configuration is erased.

**Step 5** You can now install the replacement certificate in the same manner as an original certificate. For detailed steps, see Installing a Cisco Secure ACS Server Certificate, page 10-35.



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

# Logs and Reports

Cisco Secure ACS for Windows Server produces a variety of logs and provides a way to view most of these logs in the Cisco Secure ACS HTML interface as HTML reports.

This chapter contains the following topics:


- Logging Formats, page 11-2
- Special Logging Attributes, page 11-2
- NAC Attributes in Logs, page 11-4
- Update Packets in Accounting Logs, page 11-5
- About Cisco Secure ACS Logs and Reports, page 11-6
- Working with CSV Logs, page 11-15
- Working with ODBC Logs, page 11-21
- Remote Logging, page 11-26
- Service Logs, page 11-31




Downloaded from www.Manualslib.com manuals search engine

# Logging Formats

Cisco Secure ACS logs a variety of user and system activities. Depending on the log, and how you have configured Cisco Secure ACS, logs can be recorded in one of two formats:

- **Comma-separated value (CSV) files**—The CSV format records data in columns separated by commas. This format is easily imported into a variety of third-party applications, such as Microsoft Excel or Microsoft Access. After data from a CSV file is imported into such applications, you can prepare charts or perform queries, such as determining how many hours a user was logged in to the network during a given period. For information about how to use a CSV file in a third-party application such as Microsoft Excel, please see the documentation supplied by the third-party vendor. You can access the CSV files either on the Cisco Secure ACS server hard drive or by downloading the CSV file from the HTML interface. For more information about downloading the CSV file from the HTML interface, see Viewing a CSV Report, page 11-18.
- **ODBC-compliant database tables**—ODBC logging enables you to configure Cisco Secure ACS to log directly in an ODBC-compliant relational database, where it is stored in tables, one table per log. After the data is exported to the relational database, you can use the data however you need. For more information about querying the data in your relational database, refer to the documentation supplied by the relational database vendor.

For information about the formats available for a specific log, see About Cisco Secure ACS Logs and Reports, page 11-6.

# Special Logging Attributes

Among the many attributes that Cisco Secure ACS can record in its logs, a few are of special importance. The following list explains the special logging attributes provided by Cisco Secure ACS.

- **User Attributes**—These logging attributes appear in the Attributes list for any log configuration page. Cisco Secure ACS lists them using their default names: Real Name, Description, User Field 3, User Field 4, and User Field 5. If you change the name of a user-defined attribute, the default name rather than the new name still appears in the Attributes list.



Downloaded from www.Manualslib.com manuals search engine

The content of these attributes is determined by the values entered in the corresponding fields in the user account. For more information about user attributes, see User Data Configuration Options, page 3-3.

- **ExtDB Info**—If the user is authenticated with an external user database, this attribute contains a value returned by the database. In the case of a Windows user database, this attribute contains the name of the domain that authenticated the user.

  In entries in the Failed Attempts log, this attribute contains the database that last successfully authenticated the user. It does not list the database that failed the user authentication attempt.

- **Access Device**—The name of the AAA client sending the logging data to Cisco Secure ACS.

- **Network Device Group**—The network device group to which the access device (AAA client) belongs.

- **Filter Information**—The result of network access restrictions (NARs) applied to the user, if any. The message in this field indicates whether all applicable NARs permitted the user access, all applicable NARs denied the user access, or more specific information about which NAR denied the user access. If no NARs apply to the user, this logging attribute notes that no NARs were applied.

  The Filter Information attribute is available for Passed Authentication and Failed Attempts logs.

- **Device Command Set**—The name of the device command set, if any, that was used to satisfy a command authorization request.

  The Device Command Set attribute is available for Failed Attempts logs.

- **Remote Logging Result**—Whether a forwarded accounting packet is successfully processed by a remote logging service. This attribute is useful for determining which accounting packets, if any, may not have been logged by a central logging service. It is dependent upon the receipt of an acknowledgment message from the remote logging service. The acknowledgment message indicates that the remote logging service properly processed the accounting packet in the manner that the remote logging service is configured to do. A value of `Remote-logging-successful` indicates that the remote logging service successfully processed the accounting packet. A value of `Remote-logging-failed` indicates that the remote logging service did not process the accounting packet successfully.



Downloaded from www.Manualslib.com manuals search engine

**Note** Cisco Secure ACS cannot determine how a remote logging service is configured to process accounting packets that it is forwarded. For example, if a remote logging service is configured to discard accounting packets, it discards a forwarded accounting packet and responds to Cisco Secure ACS with an acknowledgment message, causing Cisco Secure ACS to write a value of `Remote-logging-successful` in the Remote Logging Result attribute in the local log that records the account packet.

- **Application-Posture-Token**—The application posture token (APT) returned by a particular policy during a posture validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs. For more information, see NAC Attributes in Logs, page 11-4.
- **System-Posture-Token**—The system posture token (SPT) returned by a Network Admission Control (NAC) database during a posture validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs. For more information, see NAC Attributes in Logs, page 11-4.
- **Other posture validation attributes**—Attributes sent to Cisco Secure ACS by a NAC client in a posture validation request, identified by the vendor name, application name, and attribute name that uniquely identify the attribute. For example, the NAI:AV:DAT-Date attribute is an attribute containing information about the date of the DAT file on the NAC client for a Network Associates, Inc., anti-virus application. These attributes are available only in the Passed Authentications and Failed Attempts logs. For more information, see NAC Attributes in Logs, page 11-4.

# NAC Attributes in Logs

Posture validation attributes, used by NAC, can be used in the Passed Authentications and Failed Attempts logs. All inbound attributes are available for logging. The only two outbound attributes that you can record in logs are Application-Posture-Token and System-Posture-Token.



Downloaded from www.Manualslib.com manuals search engine

Posture validation requests resulting in an system posture token (SPT) of Healthy are logged in the Passed Authentications log. Posture validation requests resulting in an SPT of anything other than Healthy are logged in the Failed Attempts log. For more information about posture tokens, see Posture Tokens, page 14-4.

# Update Packets in Accounting Logs

Whenever you configure Cisco Secure ACS to record accounting data for user sessions, Cisco Secure ACS records start and stop packets. If you want, you can configure Cisco Secure ACS to record update packets, too. In addition to providing interim accounting information during a user session, update packets drive password expiry messages via CiscoSecure Authentication Agent. In this use, the update packets are referred to as watchdog packets.

**Note** To record update packets in Cisco Secure ACS accounting logs, you must configure your AAA clients to send the update packets. For more information about configuring your AAA client to send update packets, refer to the documentation for your AAA clients.

- **Logging Update Packets Locally**—To log update packets according to local Cisco Secure ACS logging configuration, enable the Log Update/Watchdog Packets from this Access Server option for each AAA client in Network Configuration.

  For more information on setting this option for a AAA client, see Adding a AAA Client, page 4-16.

- **Logging Update Packets Remotely**—To log update packets on a remote logging server, enable the Log Update/Watchdog Packets from this remote AAA Server option for the remote server AAA Server table entry on the local Cisco Secure ACS.

  For more information on setting this option for a AAA server, see Adding a AAA Server, page 4-24.



Downloaded from www.Manualslib.com manuals search engine

# About Cisco Secure ACS Logs and Reports

The logs that Cisco Secure ACS provides can be divided into four types:

- Accounting logs
- Dynamic Cisco Secure ACS administration reports
- Cisco Secure ACS system logs
- Service logs

This section contains information about the first three types of logs. For information about service logs, see Service Logs, page 11-31.

This section contains the following topics:

- Accounting Logs, page 11-6
- Dynamic Administration Reports, page 11-9
- Cisco Secure ACS System Logs, page 11-13

## Accounting Logs

Accounting logs contain information about the use of remote access services by users. By default, these logs are available in CSV format. With the exception of the Passed Authentications log, you can also configure Cisco Secure ACS to export the data for these logs to an ODBC-compliant relational database that you configure to store the log data. Table 11-1 describes all accounting logs.

In the HTML interface, all accounting logs can be enabled, configured, and viewed. Table 11-2 contains information about what you can do in the Cisco Secure ACS HTML interface regarding accounting logs.



Downloaded from www.Manualslib.com manuals search engine

*Table 11-1 Accounting Log Descriptions*

| Log | Description |
|---|---|
| TACACS+ Accounting | Contains the following information:<br>• User sessions stop and start times<br>• AAA client messages with username<br>• Caller line identification (CLID) information<br>• Session duration |
| TACACS+ Administration | Lists configuration commands entered on a AAA client using TACACS+ (Cisco IOS). Particularly if you use Cisco Secure ACS to perform command authorization, we recommend that you use this log.<br>**Note** To use the TACACS+ Administration log, you must configure TACACS+ AAA clients to perform command accounting with Cisco Secure ACS. |
| RADIUS Accounting | Contains the following information:<br>• User sessions stop and start times<br>• AAA client messages with username<br>• Caller line identification information<br>• Session duration<br>You can configure Cisco Secure ACS to include accounting for Voice-over-IP (VoIP) in the RADIUS Accounting log, in a separate VoIP accounting log, or in both places. |
| VoIP Accounting | Contains the following information:<br>• VoIP session stop and start times<br>• AAA client messages with username<br>• CLID information<br>• VoIP session duration<br>You can configure Cisco Secure ACS to include accounting for VoIP in this separate VoIP accounting log, in the RADIUS Accounting log, or in both places. |



Downloaded from www.Manualslib.com manuals search engine

*Table 11-1 Accounting Log Descriptions (continued)*

| Log | Description |
|---|---|
| Failed Attempts | Lists authentication and authorization failures with an indication of the cause. For posture validation requests, this log records the results of any posture validation that returns a posture token other than Healthy.<br>**Note** In entries in the Failed Attempts log, the ExtDB Info attribute contains the database that last successfully authenticated the user. It does not list the database that failed the user authentication attempt. |
| Passed Authentications | Lists successful authentication requests. This log is not dependent upon accounting packets from your AAA clients, so it is available even if your AAA clients do not support RADIUS accounting or if you have disabled accounting on your AAA clients. For posture validation requests, this log records the results of any posture validation that returns a posture token of Healthy.<br>**Note** The Passed Authentications log cannot be configured using an ODBC format. |

*Table 11-2 What You Can Do with Accounting Logs*

| What You Can Do | Description and Related Topics |
|---|---|
| Enable an accounting log | You can enable the log in either CSV or ODBC format.<br>• **CSV**—For instructions on how to enable an accounting log in CSV format, see Enabling or Disabling a CSV Log, page 11-17.<br>• **ODBC**—For instructions on how to enable an account log in ODBC format, see Configuring an ODBC Log, page 11-23. |



Downloaded from www.Manualslib.com manuals search engine

*Table 11-2 What You Can Do with Accounting Logs (continued)*

| What You Can Do | Description and Related Topics |
|---|---|
| View an accounting report | For instructions on viewing an accounting report in the HTML interface, see Viewing a CSV Report, page 11-18. |
| Configure an accounting log | The steps for configuring an accounting log vary depending upon which format you want to use. For more information about log formats, see Logging Formats, page 11-2.<br>• **CSV**—For instructions on configuring the CSV accounting log, see Configuring a CSV Log, page 11-19.<br>• **ODBC**—For instructions on configuring ODBC accounting log, see Configuring an ODBC Log, page 11-23. |

# Dynamic Administration Reports

These reports show the status of user accounts at the moment you access them in the Cisco Secure ACS HTML interface. They are available only in the HTML interface, are always enabled, and require no configuration.

Table 11-3 contains descriptions of all dynamic administration reports and information about what you can do regarding dynamic administration reports.



Downloaded from www.Manualslib.com manuals search engine

*Table 11-3 Dynamic Administration Report Descriptions and Related Topics*

| Report | Description and Related Topics |
|---|---|
| Logged-In Users | Lists all users receiving services for a single AAA client or all AAA clients. Users accessing the network with Cisco Aironet equipment appear on the list for the access point that they are currently associated with, provided that the firmware image on the Cisco Aironet Access Point supports sending the RADIUS Service-Type attribute for rekey authentications.<br><br>On a computer configured to perform machine authentication, machine authentication occurs when the computer started. When a computer is started and before a user logs in on that computer, the computer appears on the Logged-In Users List in the Reports and Activity section. Once user authentication begins, the computer no longer appears on the Logged-In Users List. For more information about machine authentication, see EAP and Windows Authentication, page 13-15.<br><br>**Note** To use the logged-in user list feature, you must configure AAA clients to perform authentication and accounting using the same protocol—either TACACS+ or RADIUS.<br><br>For instructions on viewing the Logged-in User report in the HTML interface, see Viewing the Logged-in Users Report, page 11-10.<br><br>For instructions about deleting logged-in users from specific AAA clients or from all AAA clients, see Deleting Logged-in Users, page 11-11. |
| Disabled Accounts | Lists all user accounts that are disabled and the reason they were disabled.<br><br>For instructions on viewing the Disabled Accounts report in the HTML interface, see Viewing the Disabled Accounts Report, page 11-12. |

## Viewing the Logged-in Users Report

To view the Logged-in Users report, follow these steps:

**Step 1** In the navigation bar, click **Reports and Activity**.

**Step 2** Click **Logged-in Users**.

The Select a AAA Client page displays the name of each AAA client, its IP address, and the number of users logged in through the AAA client. At the bottom of the table, the All AAA Clients entry shows the total number of users logged in.



Downloaded from www.Manualslib.com manuals search engine

**Tip** You can sort the table by any column's entries, in either ascending or descending order. Click a column title once to sort the table by the entries in that column in ascending order. Click the column a second time to sort the table by the entries in that column in descending order.

**Step 3** Do one of the following:

- To see a list of all users logged in, click **All AAA Clients**.
- To see a list of users logged in through a particular AAA client, click the name of the AAA client.

Cisco Secure ACS displays a table of users logged in, including the following information:

- Date and Time
- User
- Group
- Assigned IP
- Port
- Source AAA Client

**Tip** You can sort the table by the entries in any column, in either ascending or descending order. Click a column title once to sort the table by the entries in that column, in ascending order. Click the column a second time to sort the table by the entries that column in descending order.

## Deleting Logged-in Users

From a Logged-in Users Report, you can instruct Cisco Secure ACS to delete users logged into a specific AAA client. When a user session terminates without a AAA client sending an accounting stop packet to Cisco Secure ACS, the Logged-in Users Report continues to show the user. Deleting logged-in users from a AAA client ends the accounting for those user sessions.



Downloaded from www.Manualslib.com manuals search engine

**Note** Deleting logged-in users only ends the Cisco Secure ACS accounting record of users logged in to a particular AAA client. It does not terminate active user sessions, nor does it affect user records.

To delete logged-in users, follow these steps:

**Step 1** In the navigation bar, click **Reports and Activity**.

**Step 2** Click **Logged-in Users**.

The Select a AAA Client page displays the name of each AAA client, its IP address, and the number of users logged in through the AAA client. At the bottom of the table, the All AAA Clients entry shows the total number of users logged in.

**Step 3** Click the name of the AAA client whose users you want to delete from the Logged-in Users report.

Cisco Secure ACS displays a table of all users logged in through the AAA client. The Purge Logged in Users button appears below the table.

**Step 4** Click **Purge Logged in Users**.

Cisco Secure ACS displays a message, indicating the number of users purged from the report and the IP address of the AAA client.

## Viewing the Disabled Accounts Report

To view the Disabled Accounts report, follow these steps:

**Step 1** In the navigation bar, click **Reports and Activity**.

**Step 2** Click **Disabled Accounts**.

The Select a user account to edit page displays disabled user accounts, the account status, and the group to which the user account is assigned.

**Step 3** To edit a user account listed, in the User column, click the username.

Cisco Secure ACS opens the user account for editing.



Downloaded from www.Manualslib.com manuals search engine

For more information about editing a user account, see Basic User Setup Options, page 7-3.

# Cisco Secure ACS System Logs

System logs are logs about the Cisco Secure ACS system and therefore record system-related events. These logs are useful for troubleshooting or audits. They are always enabled and are only available in CSV format. Some system logs can be configured. For information about each system log, including which system logs are configurable, see Table 11-4.

For instructions on viewing a CSV report in the HTML interface, see Viewing a CSV Report, page 11-18.

***Table 11-4 Accounting Log Descriptions and Related Topics***

| Log | Description and Related Topics |
|---|---|
| ACS Backup and Restore | Lists Cisco Secure ACS backup and restore activity. This log cannot be configured. |
| RDBMS Synchronization | Lists RDBMS Synchronization activity. This log cannot be configured. |
| Database Replication | Lists database replication activity. This log cannot be configured. |
| Administration Audit | Lists actions taken by each system administrator, such as adding users, editing groups, configuring a AAA client, or viewing reports.<br>For instructions on configuring the Administration Audit log, see Configuring the Administration Audit Log, page 11-14. |



Downloaded from www.Manualslib.com manuals search engine

*Table 11-4 Accounting Log Descriptions and Related Topics (continued)*

| Log | Description and Related Topics |
|---|---|
| User Password Changes | Lists user password changes initiated by users, regardless of which password change mechanism was used to change the password. Thus, this log contains records of password changes accomplished by the CiscoSecure Authentication Agent, by the User Changeable Password HTML interface, or by Telnet session on a network device using TACACS+. It does not list password changes made by an administrator in the Cisco Secure ACS HTML interface.<br>For information about configuring the User Password Changes log, see Configuring Local Password Management, page 8-7. |
| ACS Service Monitoring | Lists when Cisco Secure ACS services start and stop.<br>For information about configuring the ACS Service Monitoring log, see Cisco Secure ACS Active Service Management, page 8-17. |

## Configuring the Administration Audit Log

You use this procedure to configure how often, or at what size limit, Cisco Secure ACS generates a new Administration Audit Log file. You can also use this procedure to configure the Administration Audit Log file storage limits with regard to number or age.

To configure the Administrative Audit log, follow these steps:

**Step 1** In the navigation bar, click **Administration Control**.

**Step 2** Click **Audit Policy**.

The Audit Policy Setup page appears.

**Step 3** To generate a new Administrative Audit CSV file at a regular interval, select one of the following options:

- **Every day**—Cisco Secure ACS generates a new Administrative Audit CSV file at the start of each day.
- **Every week**—Cisco Secure ACS generates a new Administrative Audit CSV file at the start of each week.
- **Every month**—Cisco Secure ACS generates a new Administrative Audit CSV file at the start of each month.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** To generate a new Administrative Audit CSV file when the current file reaches a specific size, select the **When size is greater than** *X* **KB** option and type the file size threshold in kilobytes in the *X* box.

**Step 5** To manage which Administrative Audit CSV files Cisco Secure ACS keeps, follow these steps:

a. Select the **Manage Directory** check box.

b. To limit the number of Administrative Audit CSV files Cisco Secure ACS retains, select the **Keep only the last** *X* **files** option and type in the *X* box the number of files you want Cisco Secure ACS to retain.

c. To limit how old Administrative Audit CSV files retained by Cisco Secure ACS can be, select the **Delete files older than** *X* **days** option and type the number of days for which Cisco Secure ACS should retain a Administrative Audit CSV file before deleting it.

**Step 6** Click **Submit**.

Cisco Secure ACS saves and implements the Administrative Audit log settings you specified.

# Working with CSV Logs

This section contains the following topics:


- CSV Log File Names, page 11-15
- CSV Log File Locations, page 11-16
- Enabling or Disabling a CSV Log, page 11-17
- Viewing a CSV Report, page 11-18
- Configuring a CSV Log, page 11-19


## CSV Log File Names

When you access a report in Reports and Activity, Cisco Secure ACS lists the CSV files in chronological order, with the current CSV file at the top of the list. The current file is named *log*.csv, where *log* is the name of the log.



Downloaded from www.Manualslib.com manuals search engine

Older files are named in the following format:

*log*`yyyy-mm-dd.csv`

where

*log* is the name of the log.

*yyyy* is the year the CSV file was started.

*mm* is the month the CSV file was started, in numeric characters.

*dd* is the date the CSV file was started.

For example, a Database Replication log file that was generated on October 13, 2002, would be named `Database Replication 2002-10-13.csv`.

# CSV Log File Locations

By default, Cisco Secure ACS keeps log files in directories unique to the log. The HTML interface enables you to configure the log file location for some logs while the location for other log files is not configurable. The default directories for all logs are within *sysdrive*`:\Program Files\CiscoSecure ACS v`*x.x*. For the subdirectory of this location for a specific log, see Table 11-5.

***Table 11-5 Default CSV Log File Locations***

| Log | Default Location | Configurable? |
|---|---|---|
| TACACS+ Accounting | `Logs\TACACS+Accounting` | Yes |
| CSV TACACS+ Administration | `Logs\TACACS+Administration` | Yes |
| CSV RADIUS Accounting | `Logs\RADIUS Accounting` | Yes |
| CSV VoIP Accounting | `Logs\VoIP Accounting` | Yes |
| CSV Failed Attempts | `Logs\Failed Attempts` | Yes |
| Passed Authentications | `Logs\Passed Authentications` | Yes |
| Cisco Secure ACS Backup and Restore | `Logs\Backup and Restore` | No |
| RDBMS Synchronization | `Logs\DbSync` | No |
| RDBMS Synchronization | `Logs\DBReplicate` | No |
| Administration Audit | `Logs\AdminAudit` | No |



Downloaded from www.Manualslib.com manuals search engine

*Table 11-5 Default CSV Log File Locations (continued)*

| Log | Default Location | Configurable? |
|---|---|---|
| User Password Changes | `CSAuth\PasswordLogs` | No |
| Cisco Secure ACS Active Service Monitoring | `Logs\ServiceMonitoring` | No |

# Enabling or Disabling a CSV Log

This procedure describes how to enable or disable a CSV log. For instructions about configuring the content of a CSV log, see Configuring a CSV Log, page 11-19.

**Note** Some CSV logs are always enabled. For information about specific logs, including whether you can disable them, see About Cisco Secure ACS Logs and Reports, page 11-6.

To enable or disable a CSV log, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Logging**.

**Step 3** Click the name of the CSV log you want to enable.

The CSV *log* Comma-Separated Values File Configuration page appears, where *log* is the name of the CSV log you selected.

**Step 4** To enable the log, under Enable Logging, select the **Log to CSV** *log* **report** check box, where *log* is the name of the CSV log you selected in Step 3.

**Step 5** To disable the log, under Enable Logging, clear the **Log to CSV** *report* **log** check box, where *log* is the name of the CSV log you selected in Step 3.

**Step 6** Click **Submit**.

If you enabled the log, Cisco Secure ACS begins logging information for the log selected. If you disabled the log, Cisco Secure ACS stops logging information for the log selected.



Downloaded from www.Manualslib.com manuals search engine

# Viewing a CSV Report

When you select Logged-in Users or Disabled Accounts, a list of logged-in users or disabled accounts appears in the display area, which is the frame on the right side of the web browser. For all other types of reports, a list of applicable reports appears. Files are listed in chronological order, with the most recent file at the top of the list. The reports are named and listed by the date on which they were created; for example, a report ending with `2002-10-13.csv` was created on October 13, 2002.

Files in CSV format can be imported into spreadsheets using most popular spreadsheet application software. Refer to your spreadsheet software documentation for instructions. You can also use a third-party reporting tool to manage report data. For example, aaa-reports! by Extraxi supports Cisco Secure ACS (http://www.extraxi.com).

You can download the CSV file for any CSV report you view in Cisco Secure ACS. The procedure below includes steps for doing so.

To view a CSV report, follow these steps:

**Step 1** In the navigation bar, click **Reports and Activity**.

**Step 2** Click the name of the CSV report you want to view.

On the right side of the browser, Cisco Secure ACS lists the current CSV report filename and the filenames of any old CSV report files.

**Tip** You can configure how Cisco Secure ACS handles old CSV report files. For more information, see Configuring a CSV Log, page 11-19.

**Step 3** Click the CSV report filename whose contents you want to view.

If the CSV report file contains information, the information appears in the display area.

**Tip** You can sort the table by any entries in the column, in either ascending or descending order. Click a column title once to sort the table by that column's entries in ascending order. Click the column a second time to sort the table by the entries in that column in descending order.



Downloaded from www.Manualslib.com manuals search engine

**Tip** To check for newer information in the current CSV report, click **Refresh**.

**Step 4** If you want to download the CSV log file for the report you are viewing, follow these steps:

a. Click **Download**.

Your browser displays a dialog box for accepting and saving the CSV file.

b. Choose a location to save the CSV file and save the file.

# Configuring a CSV Log

This procedure describes how to configure the content of a CSV log. For instructions to enable or disable a CSV log, see Enabling or Disabling a CSV Log, page 11-17.

The logs to which this procedure applies are as follows:

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Failed Attempts
- Passed Authentications

**Note** The ACS Backup and Restore, RDBMS Synchronization, and Database Replication CSV logs cannot be configured.

You can configure several aspects of a CSV log:

- **Log content**—You can select which data attributes are included in the log.
- **Log generation frequency**—You can determine whether a new log is started after a specific length of time or when the current CSV file reaches a particular size.



Downloaded from www.Manualslib.com manuals search engine

- **CSV file location**—You can specify where on the local hard drive Cisco Secure ACS writes the CSV file.
- **CSV file retention**—You can specify how many old CSV files Cisco Secure ACS maintains or set a maximum number of files it is to retain.

To configure a CSV log, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Logging**.

**Step 3** Click the name of the CSV log you want to enable.

The CSV *log* Comma-Separated Values File Configuration page appears, where *log* is the name of the CSV log you selected.

The Select Columns To Log table contains two lists, Attributes and Logged Attributes. The attributes in the Logged Attributes list appear on the log selected.

**Step 4** To add an attribute to the log, select the attribute in the Attributes list, and then click **-->** (right arrow button).

The attribute moves to the Logged Attributes list.

**Tip** Use the vertical scroll bar to find attributes not visible in the list box.

**Step 5** To remove an attribute from the log, select the attribute in the Logged Attributes list, and then click **<--** (left arrow button).

The attribute moves to the Attributes list.

**Tip** Use the vertical scroll bar to find attributes not visible in the list.

**Step 6** To set the attributes in the Logged Attributes list back to the default selections, at the bottom of the browser window, click **Reset Columns**.



Downloaded from www.Manualslib.com manuals search engine

**Step 7** To generate a new CSV file at a regular interval, select one of the following options:

- **Every day**—Cisco Secure ACS generates a new CSV file at the start of each day.
- **Every week**—Cisco Secure ACS generates a new CSV file at the start of each week.
- **Every month**—Cisco Secure ACS generates a new CSV file at the start of each month.

**Step 8** To generate a new CSV file when the current file reaches a specific size, select the **When size is greater than** *X* **KB** option and type the file size threshold, in kilobytes, in the *X* box.

**Step 9** To manage which CSV files Cisco Secure ACS keeps, follow these steps:

a. Select the **Manage Directory** check box.

b. To limit the number of CSV files Cisco Secure ACS retains, select the **Keep only the last** *X* **files** option and type the number of files you want Cisco Secure ACS to retain in the *X* box.

c. To limit how old CSV files retained by Cisco Secure ACS can be, select the **Delete files older than** *X* **days** option and type the number of days for which Cisco Secure ACS should retain a CSV file before deleting it.

**Step 10** Click **Submit**.

Cisco Secure ACS implements the CSV log configuration that you specified.

# Working with ODBC Logs

This section contains the following topics:

- Preparing for ODBC Logging, page 11-22
- Configuring a System Data Source Name for ODBC Logging, page 11-22
- Configuring an ODBC Log, page 11-23



Downloaded from www.Manualslib.com manuals search engine

# Preparing for ODBC Logging

To prepare for ODBC logging, there are several steps you must complete. After you have prepared for ODBC logging, you can configure individual ODBC logs.

To prepare for ODBC logging, follow these steps:

**Step 1** Set up the relational database to which you want to export logging data. For more information, refer to your relational database documentation.

**Step 2** Set up a system data source name (DSN) on the computer running Cisco Secure ACS. For instructions, see Configuring a System Data Source Name for an ODBC External User Database, page 13-70.

**Step 3** Enable ODBC logging in the Cisco Secure ACS HTML interface:

a. In the navigation bar, click **Interface Configuration**.

b. Click **Advanced Options**.

c. Select the **ODBC Logging** check box.

d. Click **Submit**.

Cisco Secure ACS enables the ODBC logging feature. On the Logging page, in the System Configuration section, Cisco Secure ACS displays links for configuring ODBC logs.

You can now configure individual ODBC logs. For instructions, see Configuring an ODBC Log, page 11-23.

# Configuring a System Data Source Name for ODBC Logging

On the computer running Cisco Secure ACS, you must create a system DSN for Cisco Secure ACS to communicate with the relational database that is to store your logging data.

To create a system DSN for use with ODBC logging, follow these steps:

**Step 1** In Windows Control Panel, double-click **ODBC Data Sources**.

**Step 2** In the ODBC Data Source Administrator page, click the **System DSN** tab.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** Click **Add**.

**Step 4** Select the driver you need to use with your new DSN, and then click **Finish**.

A dialog box displays fields requiring information specific to the ODBC driver you selected.

**Step 5** Type a descriptive name for the DSN in the Data Source Name box.

**Step 6** Complete the other fields required by the ODBC driver you selected. These fields may include information such as the IP address of the server on which the ODBC-compliant relational database runs.

**Step 7** Click **OK**.

**Step 8** Close the ODBC window and Windows Control Panel.

The System DSN to be used by Cisco Secure ACS for communicating with the relational database is created on the computer running Cisco Secure ACS. The name you assigned to the DSN appears in the Data Source list on each ODBC log configuration page.

# Configuring an ODBC Log

The logs to which this procedure applies are as follows:

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Failed Attempts

**Note** Before you can configure an ODBC log, you must prepare for ODBC logging. For more information, see Preparing for ODBC Logging, page 11-22.



Downloaded from www.Manualslib.com manuals search engine

To configure an ODBC log, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Logging**.

**Step 3** Click the name of the ODBC log you want to enable.

The ODBC *log* Configuration page appears, where *log* is the name of the ODBC log you selected.

The Select Columns To Log table contains two lists: Attributes and Logged Attributes. When you first access the ODBC configuration page for a log, the Logged Attributes list contains the default set of attributes. Cisco Secure ACS includes in the log only those attributes that are in the Logged Attributes list.

**Step 4** Specify the attributes that you want Cisco Secure ACS to send to the relational database:

**a.** To add an attribute to the log, select the attribute in the Attributes list, and then click **-->** (right arrow button).

The attribute moves to the Logged Attributes list.

**Tip** Use the vertical scroll bar to find attributes not visible in the list box.

**b.** To remove an attribute from the log, select the attribute in the Logged Attributes list, and then click **<--** (left arrow button).

The attribute moves to the Attributes list.

**Tip** Use the vertical scroll bar to find attributes not visible in the list box.

**c.** To set the attributes in the Logged Attributes list back to the default selections, click **Reset Columns**.

**Step 5** In the ODBC Connection Settings table, configure Cisco Secure ACS to communicate with the ODBC database. To do so, follow these steps:

**a.** From the Data Source list, select the system DSN you created to allow Cisco Secure ACS to send ODBC logging data to your relational database.

**b.** In the Username box, type the username of a user account in your relational database (up to 80 characters).



Downloaded from www.Manualslib.com manuals search engine

**Note** The user must have sufficient privileges in the relational database to write the ODBC logging data to the appropriate table.

c. In the Password box, type the password (up to 80 characters) for the relational database user account you specified in Step b.

d. In the Table Name box, type the name (up to 80 characters) of the table to which you want ODBC logging data appended.

**Step 6** Click **Submit**.

Cisco Secure ACS saves the log configuration.

**Step 7** Click the name of the ODBC log you are configuring.

Cisco Secure ACS displays the ODBC log configuration page again.

**Step 8** Click **Show Create Table**.

The right side of the browser displays an SQL create table statement for Microsoft SQL Server. The table name is the name specified in the Table Name box. The column names are the attributes specified in the Logged Attributes list.

**Note** The generated SQL is valid for Microsoft SQL Server only. If you are using another relational database, refer to your relational database documentation for information about writing a command to create a table.

**Step 9** Using the information provided in the generated SQL, create a table in your relational database for this ODBC log.

**Note** For ODBC logging to work, the table name and the column names must match exactly the names in the generated SQL.

**Step 10** Continuing in Cisco Secure ACS, access the configuration page for the ODBC log you are configuring:

a. In the navigation bar, click **System Configuration**.

b. Click **Logging**.



Downloaded from www.Manualslib.com manuals search engine

c. Click the name of the ODBC log you are configuring.

The ODBC *log* Configuration page appears, where *log* is the name of the ODBC log you selected.

**Step 11** Select the **Log to ODBC** *log* **report** check box, where *log* is the name of the ODBC log you selected.

**Step 12** Click **Submit**.

Cisco Secure ACS begins sending logging data to the relational database table specified, using the system DSN you configured.

# Remote Logging

This section discusses remote logging capabilities of Cisco Secure ACS.

This section contains the following topics:


- About Remote Logging, page 11-26
- Implementing Centralized Remote Logging, page 11-27
- Remote Logging Options, page 11-28
- Enabling and Configuring Remote Logging, page 11-29
- Disabling Remote Logging, page 11-31


## About Remote Logging

The Remote Logging feature enables you to centralize accounting logs generated by multiple Cisco Secure ACSes. You can configure each Cisco Secure ACS to point to one Cisco Secure ACS that is to be used as a central logging server. The central logging Cisco Secure ACS still performs AAA functions, but it also is the repository for accounting logs it receives. For more information about Cisco Secure ACS accounting logs, see Accounting Logs, page 11-6.

The Remote Logging feature enables Cisco Secure ACS to send accounting data received from AAA clients directly to the CSLog service on the remote logging server, where the accounting data is written to the logs. The logging server



Downloaded from www.Manualslib.com manuals search engine

generates the accounting logs in the formats it is configured to use—CSV and ODBC—regardless of the local logging configuration on the Cisco Secure ACSes sending the data to the central logging server.

Cisco Secure ACS listens on TCP port 2001 for remote logging communication. Remote logging data is encrypted by a 128-bit proprietary algorithm.

**Note** The Remote Logging feature does not affect the forwarding of accounting data for proxied authentication requests. Cisco Secure ACS only applies Remote Logging settings to accounting data for sessions authenticated by proxy when accounting data for sessions authenticated by proxy is logged locally. For more information about proxied authentication requests and accounting data for sessions authenticated by proxy, see Proxy Distribution Table Configuration, page 4-34.

# Implementing Centralized Remote Logging

### Before You Begin

Make sure that gateway devices between remote Cisco Secure ACSes and the central logging Cisco Secure ACS permit the central logging Cisco Secure ACS to receive data on TCP port 2001.

To implement centralized remote logging, follow these steps:

**Step 1** On a computer that you want to use to store centralized logging data, install Cisco Secure ACS for Windows Server. For information about installing Cisco Secure ACS, see the *Installation Guide for Cisco Secure ACS for Windows Server*.

**Step 2** In the Cisco Secure ACS running on the central logging server, follow these steps:

**a.** Configure the accounting logs as needed. All accounting data sent to the central logging server will be recorded in the way you configure accounting logs on this Cisco Secure ACS. For information about accounting logs, see Accounting Logs, page 11-6.

Accounting logs can be recorded in either CSV or ODBC format. For information about configuring CSV logs, see Working with CSV Logs, page 11-15. For information about configuring ODBC logs, see Configuring an ODBC Log, page 11-23.



Downloaded from www.Manualslib.com manuals search engine

b. Add to the AAA Servers table each Cisco Secure ACS that the central logging server is to receive accounting data from. For more information, see AAA Server Configuration, page 4-21.

**Note** If the central logging server is to log watchdog and update packets for a Cisco Secure ACS, be sure that the Log Update/Watchdog Packets from this remote AAA Server check box is selected for that Cisco Secure ACS in the AAA Servers table.

**Step 3** For each Cisco Secure ACS that is to send its accounting data to the central logging server, follow these steps:

a. Add the central logging server to the AAA Servers table in Network Configuration. For more information, see AAA Server Configuration, page 4-21.

b. Enable remote logging. For more information, see Enabling and Configuring Remote Logging, page 11-29.

**Step 4** If you want to create other central logging servers, for use either as secondary servers or as mirrored logging servers, perform Step 1 through Step 3 for each additional server.

# Remote Logging Options

Cisco Secure ACS provides the remote logging options listed below. These options appear on the Remote Logging Setup page.

- **Do not log Remotely**—Cisco Secure ACS writes accounting data for locally authenticated sessions only to the local logs that are enabled.
- **Log to all selected remote log services**—Cisco Secure ACS sends accounting data for locally authenticated sessions to all Cisco Secure ACSes in the Selected Log Services list.
- **Log to subsequent remote log services on failure**—Cisco Secure ACS sends accounting data for locally authenticated sessions to the first Cisco Secure ACS that is operational in the Selected Log Services list. This



Downloaded from www.Manualslib.com manuals search engine

behavior enables you to configure one or more backup central logging servers so that no accounting data is lost if the first central logging server fails or is otherwise unavailable to Cisco Secure ACS.

- **Remote Log Services**—This list represents the Cisco Secure ACSes configured in the Remote Agents table in Network Configuration to which Cisco Secure ACS *does not* send accounting data for locally authenticated sessions.
- **Selected Log Services**—This list represents the Cisco Secure ACSes configured in the Remote Agents table in Network Configuration to which Cisco Secure ACS *does* send accounting data for locally authenticated sessions.

# Enabling and Configuring Remote Logging

**Note** Before configuring the Remote Logging feature on a Cisco Secure ACS, make sure that you have configured your central logging Cisco Secure ACS. For more information, see Implementing Centralized Remote Logging, page 11-27.

To enable and configure remote logging, follow these steps:

**Step 1** To enable the Remote Logging feature in the HTML interface, follow these steps:

a. Click **Interface Configuration**.

b. Click **Advanced Options**.

c. Select the **Remote Logging** check box.

d. Click **Submit**.

Cisco Secure ACS displays the Remote Logging link on the Logging page in the System Configuration section.

**Step 2** Click **System Configuration**.

**Step 3** Click **Logging**.

The Logging Configuration page appears.

**Step 4** Click **Remote Logging**.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** Select the applicable remote logging option:

a. To send the accounting information for this Cisco Secure ACS to more than one Cisco Secure ACS, select the **Log to all selected remote log services** option.

b. To send the accounting information for this Cisco Secure ACS to one Cisco Secure ACS, select the **Log to subsequent remote log services on failure** option.

**Note** Use the "Log to subsequent remote log services on failure" option when you want to configure Cisco Secure ACS to send accounting data to a second remote Cisco Secure ACS if the first Cisco Secure ACS fails.

**Step 6** For each remote Cisco Secure ACS you want to have in the Selected Log Services list, follow these steps:

a. In the Remote Log Services list, select the name of a Cisco Secure ACS to which you want to send accounting data for locally authenticated sessions.

**Note** The Cisco Secure ACSes available in the Remote Log Services list is determined by the AAA Servers table in Network Configuration. For more information about the AAA Servers table, see AAA Server Configuration, page 4-21.

b. Click **-->** (right arrow button) to move the selected Cisco Secure ACS to the Selected Log Services list.

**Step 7** To assign an order to the servers in the Selected Log Services list, click **Up** and **Down** to move selected Cisco Secure ACSes until you have created the order you need.

**Note** If the "Log to subsequent remote log services on failure" option is selected, Cisco Secure ACS logs to the first accessible Cisco Secure ACS in the Selected Log Services list.



Downloaded from www.Manualslib.com manuals search engine

**Step 8** Click **Submit**.

Cisco Secure ACS saves and implements the remote logging configuration you specified.

## Disabling Remote Logging

By disabling the Remote Logging feature, you prevent Cisco Secure ACS from sending its accounting information to a central logging Cisco Secure ACS.

To disable remote logging, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Logging**.

**Step 3** Click **Remote Logging**.

**Step 4** Select the **Do not log Remotely** option.

**Step 5** Click **Submit**.

Cisco Secure ACS no longer sends its accounting information for locally authenticated sessions to remote logging servers.

# Service Logs

Service logs are considered diagnostic logs and are used for troubleshooting or debugging purposes only. These logs are not intended for general use by Cisco Secure ACS administrators; instead, they are mainly sources of information for Cisco support personnel. Service logs contain a record of all Cisco Secure ACS service actions and activities. When service logging is enabled, each service generates a log whenever the service is running, whether or not you are using the service. For example, RADIUS service logs are created even if you are not using the RADIUS protocol in your network.

For more information about Cisco Secure ACS services, see Chapter 1, "Overview".



Downloaded from www.Manualslib.com manuals search engine

# Services Logged

Cisco Secure ACS generates logs for the following services:

- CSAdmin
- CSAuth
- CSDBSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

These files are located in the `\Logs` subdirectory of the applicable service directory. For example, the following is the default directory for the CiscoSecure authentication service:

`c:\Program Files\CiscoSecure ACS v`*x.x*`\CSAuth\Logs`

The most recent debug log is named as follows:

*SERVICE*`.log`

where *SERVICE* is the name of the applicable service.
Older debug logs are named with the year, month, and date they were created. For example, a file created on July 13, 1999, would be named as follows:

*SERVICE* `1999-07-13.log`

where *SERVICE* is the name of the applicable service.

If you selected the Day/Month/Year format, the file would be named as follows:

*SERVICE* `13-07-1999.log`



Downloaded from www.Manualslib.com manuals search engine

# Configuring Service Logs

You can configure how Cisco Secure ACS generates and manages the service log file. The options for configuring the service log file are listed below.

- **Level of detail**—You can set the service log file to contain one of three levels of detail:
  - **None**—No log file is generated.
  - **Low**—Only start and stop actions are logged. This is the default setting.
  - **Full**—All services actions are logged.
- **Generate new file**—You can control how often a new service log file is created:
  - **Every Day**—Cisco Secure ACS generates a new log file at 12:01 A.M. local time every day.
  - **Every Week**—Cisco Secure ACS generates a new log file at 12:01 A.M. local time every Sunday.
  - **Every Month**—Cisco Secure ACS generates a new log file at 12:01 A.M. on the first day of every month.
  - **When Size is Greater than *x* KB**—Cisco Secure ACS generates a new log file after the current service log file reaches the size specified, in kilobytes, by *x*.
- **Manage Directory**—You can control how long service log files are kept:
  - **Keep only the last *x* files**—Cisco Secure ACS retains up to the number of files specified by *x*.
  - **Delete files older than *x* days**—Cisco Secure ACS retains only those service logs that are not older than the number of days specified by *x*.

To configure how Cisco Secure ACS generates and manages the service log file, follow these steps:

**Step 1** In the navigation bar, click **System Configuration**.

**Step 2** Click **Service Control**.

The status of the services appears in the CiscoSecure ACS on *hostname* table, where *hostname* is the name of the computer running Cisco Secure ACS.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** To disable the service log file, under Level of detail, select the **None** option.

After you click Restart, Cisco Secure ACS does not generate new service logs file.

**Step 4** To configure how often Cisco Secure ACS creates a service log file, select one of the options under Generate New File.

**Note** Settings under Generate New File have no effect if you selected None under Level of detail.

**Step 5** To manage which service log files Cisco Secure ACS keeps, follow these steps:

a. Select the **Manage Directory** check box.

b. To limit the number of service log files Cisco Secure ACS retains, select the **Keep only the last** *X* **files** option and in the *X* box type the number of files you want Cisco Secure ACS to retain.

c. To limit how old service log files retained by Cisco Secure ACS can be, select the **Delete files older than** *X* **days** option and in the *X* box type the number of days for which Cisco Secure ACS should retain a service log file before deleting it.

**Step 6** Click **Restart**.

Cisco Secure ACS restarts its services and implements the service log settings you specified.



Downloaded from www.Manualslib.com manuals search engine

CHAPTER 12

# Administrators and Administrative Policy

This chapter addresses the Cisco Secure ACS Solution Engine features found in the Administration Control section of the HTML interface.

This chapter contains the following topics:


- Administrator Accounts, page 12-1
- Access Policy, page 12-11
- Session Policy, page 12-16
- Audit Policy, page 12-18


## Administrator Accounts

This section provides details about Cisco Secure ACS administrators.

This section contains the following topics:


- About Administrator Accounts, page 12-2
- Administrator Privileges, page 12-3
- Adding an Administrator Account, page 12-6
- Editing an Administrator Account, page 12-7
- Unlocking a Locked Out Administrator Account, page 12-10
- Deleting an Administrator Account, page 12-11





Downloaded from www.Manualslib.com manuals search engine

# About Administrator Accounts

Administrators are the only users of the Cisco Secure ACS HTML interface. To access the Cisco Secure ACS HTML interface from a browser run elsewhere than on the Cisco Secure ACS Windows server itself, you must log in to Cisco Secure ACS using an administrator account. If your Cisco Secure ACS is so configured, you may need to log in to Cisco Secure ACS even in a browser run on the Cisco Secure ACS Windows server. For more information about automatic local logins, see Session Policy, page 12-16.

**Note** Cisco Secure ACS administrator accounts are unique to Cisco Secure ACS. They are not related to other administrator accounts, such as Windows users with administrator privileges.

In the HTML interface, an administrator can configure any of the features provided in Cisco Secure ACS; however, the ability to access various parts of the HTML interface can be limited by revoking privileges to those parts of the HTML interface that a given administrator is not allowed to access.

For example, you may want to limit access to the Network Configuration section of the HTML interface to administrators whose responsibilities include network management. To do so, you would select only the Network Configuration privilege for applicable administrator accounts. For more information about administrator privileges, see Administrator Privileges, page 12-3.

Cisco Secure ACS administrator accounts have no correlation with Cisco Secure ACS user accounts or username and password authentication. Cisco Secure ACS stores accounts created for authentication of network service requests and those created for Cisco Secure ACS administrative access in separate internal databases.



Downloaded from www.Manualslib.com manuals search engine

# Administrator Privileges

You can grant appropriate privileges to each Cisco Secure ACS administrator by assigning privileges on an administrator-by-administrator basis. You control privileges by selecting the options from the Administrator Privileges table on the Add Administrator or Edit Administrator pages. These options are listed below:

- **User and Group Setup**—Contains the following privilege options for the User Setup and Group Setup sections of the HTML interface:
  - **Add/Edit users in these groups**—Enables the administrator to add or edit users and to assign users to the groups in the Editable groups list.
  - **Setup of these groups**—Enables the administrator to edit the settings for the groups in the Editable groups list.
  - **Available Groups**—Lists the user groups for which the administrator *does not* have edit privileges and to which the administrator *cannot* add users.
  - **Editable Groups**—Lists the user groups for which the administrator *does* have edit privileges and to which the administrator *can* add users.
- **Shared Profile Components**—Contains the following privilege options for the Shared Profile Components section of the HTML interface:
  - **Network Access Restriction Sets**—Allows the administrator full access to the Network Access Restriction Sets feature.
  - **Downloadable ACLs**—Allows the administrator full access to the Downloadable PIX ACLs feature.
  - **Create New Device Command Set Type**—Allows the administrator account to be used as valid credentials by another Cisco application for adding new device command set types. New device command set types that are added to Cisco Secure ACS using this privilege appear in the Shared Profile Components section of the HTML interface.
  - **Shell Command Authorization Sets**—Allows the administrator full access to the Shell Command Authorization Sets feature.
  - **PIX Command Authorization Sets**—Allows the administrator full access to the PIX Command Authorization Sets feature.



Downloaded from www.Manualslib.com manuals search engine

**Note** Additional command authorization set privilege options may appear, if other Cisco network management applications, such as CiscoWorks2000, have updated the configuration of Cisco Secure ACS.

- **Network Configuration**—Allows the administrator full access to the features in the Network Configuration section of the HTML interface.
- **System Configuration...—**Contains the privilege options for the features found in the System Configuration section of the HTML interface. For each of the following features, enabling the option allows the administrator full access to the feature.
  - **Service Control**—For more information about this feature, see Service Control, page 8-1.
  - **Date/Time Format Control**—For more information about this feature, see Date Format Control, page 8-3.
  - **Logging Control**—For more information about this feature, see Logging, page 8-3.
  - **Local Password Management**—For more information about this feature, see Local Password Management, page 8-5.
  - **DB Replication**—For more information about this feature, see CiscoSecure Database Replication, page 9-1.
  - **RDBMS Synchronization**—For more information about this feature, see RDBMS Synchronization, page 9-25.
  - **IP Pool Address Recovery**—For more information about this feature, see IP Pools Address Recovery, page 9-51.
  - **IP Pool Server Configuration**—For more information about this feature, see IP Pools Server, page 9-44.
  - **ACS Backup**—For more information about this feature, see Cisco Secure ACS Backup, page 8-9.
  - **ACS Restore**—For more information about this feature, see Cisco Secure ACS System Restore, page 8-14.
  - **ACS Service Management**—For more information about this feature, see Cisco Secure ACS Active Service Management, page 8-17.



Downloaded from www.Manualslib.com manuals search engine

  - **VoIP Accounting Configuration**—For more information about this feature, see VoIP Accounting Configuration, page 8-21.
  - **ACS Certificate Setup**—For more information about this feature, see Cisco Secure ACS Certificate Setup, page 10-34.
  - **Global Authentication Setup**—For more information about this feature, see Global Authentication Setup, page 10-26.
- **Interface Configuration**—Allows the administrator full access to the features in the Interface Configuration section of the HTML interface.
- **Administration Control**—Allows the administrator full access to the features in the Administration Control section of the HTML interface.
- **External User Databases**—Allows the administrator full access to the features in the External User Databases section of the HTML interface.
- **Reports & Activity**—Contains the privilege options for the reports and features found in the Reports and Activity section of the HTML interface. For each of the following features, enabling the option allows the administrator full access to the feature.
  - **TACACS+ Accounting**—For more information about this report, see Accounting Logs, page 11-6.
  - **TACACS+ Administration**—For more information about this report, see Accounting Logs, page 11-6.
  - **RADIUS Accounting**—For more information about this report, see Accounting Logs, page 11-6.
  - **VoIP Accounting**—For more information about this report, see Accounting Logs, page 11-6.
  - **Passed Authentications**—For more information about this report, see Accounting Logs, page 11-6.
  - **Failed Attempts**—For more information about this report, see Accounting Logs, page 11-6.
  - **Logged-in Users**—For more information about this report, see Dynamic Administration Reports, page 11-9.
  - **Purge of Logged-in Users**—For more information about this feature, see Deleting Logged-in Users, page 11-11.
  - **Disabled Accounts**—For more information about this report, see Dynamic Administration Reports, page 11-9.



Downloaded from www.Manualslib.com manuals search engine

- **ACS Backup and Restore**—For more information about this report, see Cisco Secure ACS System Logs, page 11-13.
- **DB Replication**—For more information about this report, see Cisco Secure ACS System Logs, page 11-13.
- **RDBMS Synchronization**—For more information about this report, see Cisco Secure ACS System Logs, page 11-13.
- **Administration Audit**—For more information about this report, see Cisco Secure ACS System Logs, page 11-13.
- **ACS Service Monitor**—For more information about this report, see Cisco Secure ACS System Logs, page 11-13.
- **User Change Password**—For more information about this report, see Cisco Secure ACS System Logs, page 11-13.

# Adding an Administrator Account

**Before You Begin**

For descriptions of the options available while adding an administrator account, see Administrator Privileges, page 12-3.

To add a Cisco Secure ACS administrator account, follow these steps:

**Step 1** In the navigation bar, click **Administration Control**.

**Step 2** Click **Add Administrator**.

The Add Administrator page appears.

**Step 3** Complete the boxes in the Administrator Details table:

a. In the Administrator Name box, type the login name (up to 32 characters) for the new Cisco Secure ACS administrator account.

b. In the Password box, type the password (up to 32 characters) for the new Cisco Secure ACS administrator account.

c. In the Confirm Password box, type the password a second time.

**Step 4** To select all privileges, including user group editing privileges for all user groups, click **Grant All**.



Downloaded from www.Manualslib.com manuals search engine

All privilege options are selected. All user groups move to the Editable groups list.

**Tip** To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

**Step 5** To grant user and user group editing privileges, follow these steps:

a. Select the desired check boxes under User & Group Setup.

b. To move a user group to the Editable groups list, select the group in the Available groups list, and then click **-->** (right arrow button).

The selected group moves to the Editable groups list.

c. To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click **<--** (left arrow button).

The selected group moves to the Available groups list.

d. To move all user groups to the Editable groups list, click **>>**.

The user groups in the Available groups list move to the Editable groups list.

e. To remove all user groups from the Editable groups list, click **<<**.

The user groups in the Editable groups list move to the Available groups list.

**Step 6** To grant any of the remaining privilege options, in the Administrator Privileges table, select the applicable check boxes.

**Step 7** Click **Submit**.

Cisco Secure ACS saves the new administrator account. The new account appears in the list of administrator accounts on the Administration Control page.

# Editing an Administrator Account

You can edit a Cisco Secure ACS administrator account to change the privileges granted to the administrator. You can effectively disable an administrator account by revoking all privileges.



Downloaded from www.Manualslib.com manuals search engine

**Note** You cannot change the name of an administrator account; however, you can delete an administrator account and then create an account with the new name. For information about deleting an administrator account, see Deleting an Administrator Account, page 12-11. For information about creating an administrator account, see Adding an Administrator Account, page 12-6.

For information about administrator privilege options, see Administrator Privileges, page 12-3.

**Before You Begin**

For descriptions of the options available while editing an administrator account, see Administrator Privileges, page 12-3.

To edit Cisco Secure ACS administrator account privileges, follow these steps:

**Step 1** In the navigation bar, click **Administration Control**.

Cisco Secure ACS displays the Administration Control page.

**Step 2** Click the name of the administrator account whose privileges you want to edit.

The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

**Step 3** To change the administrator password, follow these steps:

**a.** In the Password box, double-click the asterisks, and then type the new password (up to 32 characters) for the administrator.

The new password replaces the existing, masked password.

**b.** In the Confirm Password box, double-click the asterisks, and then type the new administrator password a second time.

The new password is effective immediately after you click Submit in Step 9.

**Step 4** If the Reset current failed attempts count check box appears below the Confirm Password box and you want to allow the administrator whose account you are editing to access the Cisco Secure ACS HTML interface, select the **Reset current failed attempts count** check box.



Downloaded from www.Manualslib.com manuals search engine

**Note** If the Reset current failed attempts count check box appears below the Confirm Password box, the administrator cannot access Cisco Secure ACS unless you complete Step 4. For more information about re-enabling an administrator account, see Unlocking a Locked Out Administrator Account, page 12-10.

**Step 5** To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

All privilege options are selected. All user groups move to the Editable groups list.

**Step 6** To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

All privileges options are cleared. All user groups move to the Available groups list.

**Step 7** To grant user and user group editing privileges, follow these steps:

**a.** Under User & Group Setup, select the applicable check boxes.

**b.** To move all user groups to the Editable groups list, click **>>**.

The user groups in the Available groups list move to the Editable groups list.

**c.** To move a user group to the Editable groups list, select the group in the Available groups list, and then click **-->** (right arrow button).

The selected group moves to the Editable groups list.

**d.** To remove all user groups from the Editable groups list, click **<<**.

The user groups in the Editable groups list move to the Available groups list.

**e.** To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click **<--** (left arrow button).

The selected group moves to the Available groups list.

**Step 8** To grant any remaining privilege options, select the applicable check boxes in the Administrator Privileges table.



Downloaded from www.Manualslib.com manuals search engine

**Step 9** To revoke any remaining privilege options, clear the applicable check boxes in the Administrator Privileges table.

**Step 10** Click **Submit**.

Cisco Secure ACS saves the changes to the administrator account.

# Unlocking a Locked Out Administrator Account

Cisco Secure ACS disables the accounts of administrators who have attempted to access the Cisco Secure ACS HTML interface and have provided an incorrect password in more successive attempts than is specified on the Session Policy Setup page. Until the failed attempts counter for a disabled administrator account is reset, the administrator cannot access the HTML interface.

For more information about configuring how many successive failed login attempts can occur before Cisco Secure ACS disables an administrator account, see Session Policy, page 12-16.

To reset the failed attempts count for an administrator, follow these steps:

**Step 1** In the navigation bar, click **Administration Control**.

Cisco Secure ACS displays the Administration Control page.

**Step 2** Click the name of the administrator account whose account you want to re-enable.

The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

If the Reset current failed attempts count check box appears below the Confirm Password box, the administrator account cannot access the HTML interface.

**Step 3** Select the **Reset current failed attempts count** check box.

**Step 4** Click **Submit**.

Cisco Secure ACS saves the changes to the administrator account.



Downloaded from www.Manualslib.com manuals search engine

## Deleting an Administrator Account

You can delete a Cisco Secure ACS administrator account when you no longer need it. We recommend deleting any unused administrator accounts.

To delete a Cisco Secure ACS administrator account, follow these steps:

**Step 1** In the navigation bar, click **Administration Control**.

Cisco Secure ACS displays the Administration Control page.

**Step 2** In the Administrators table, click the name of the administrator account that you want to delete.

The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

**Step 3** Click **Delete**.

Cisco Secure ACS displays a confirmation dialog box.

**Step 4** Click **OK**.

Cisco Secure ACS deletes the administrator account. The Administrators table on the Administration Control page no longer lists the administrator account that you deleted.

# Access Policy

The Access Policy feature affects access to the Cisco Secure ACS HTML interface. You can limit access by IP address and by the TCP port range used for administrative sessions. You can also enable secure socket layer (SSL) for access to the HTML interface.

This section contains the following topics:

- Access Policy Options, page 12-12
- Setting Up Access Policy, page 12-14



Downloaded from www.Manualslib.com manuals search engine

# Access Policy Options

You can configure the following options on the Access Policy Setup page:

- **IP Address Filtering**—Contains the following IP address filtering options:
  - **Allow all IP addresses to connect**—Allow access to the HTML interface from any IP address.
  - **Allow only listed IP addresses to connect**—Allow access to the HTML interface only from IP addresses *inside* the address range(s) specified in the IP Address Ranges table.
  - **Reject connections from listed IP addresses**—Allow access to the HTML interface only from IP addresses *outside* the address range(s) specified in the IP Address Ranges table.
- **IP Address Ranges**—The IP Address Ranges table contains ten rows for configuring IP address ranges. The ranges are always inclusive; that is, the range includes the start and end IP addresses. The IP addresses entered to define a range must differ only in the last octet (Class C format).

  The IP Address Ranges table contains one column of each of the following boxes:
  - **Start IP Address**—Defines the lowest IP address of the range specified in the current row.
  - **End IP Address**—Defines the highest IP address of the range specified in the current row.
- **HTTP Port Allocation**—Contains the following options for configuring TCP ports used for remote access to the HTML interface.
  - **Allow any TCP ports to be used for Administration HTTP Access**—Allow the ports used by administrative HTTP sessions to include the full range of TCP ports.
  - **Restrict Administration Sessions to the following port range From Port** *X* **to Port** *Y*—Restrict the ports used by administrative HTTP sessions to the range specified in the *X* and *Y* boxes, inclusive. The size of the range specified determines the maximum number of concurrent administrative sessions.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS uses port 2002 to start all administrative sessions. You do not need to include port 2002 in the port range. Also, Cisco Secure ACS does not allow you to define an HTTP port range that consists only of port 2002. Your port range must consist of at least one port other than port 2002.

A firewall configured to permit HTTP traffic over the Cisco Secure ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port a web browser must address to initiate an administrative session.

**Note** We do not recommend allowing administration of Cisco Secure ACS from outside a firewall. If you do choose to allow access to the HTML interface from outside a firewall, keep the HTTP port range as narrow as possible. This can help prevent accidental discovery of an active administrative port by unauthorized users. An unauthorized user would have to impersonate, or "spoof," the IP address of a legitimate host to make use of the active administrative session HTTP port.

- **Secure Socket Layer Setup**—The Use HTTPS Transport for Administration Access check box defines whether Cisco Secure ACS uses secure socket layer protocol to encrypt HTTP traffic between the CSAdmin service and a web browser used to access the HTML interface. When this option is enabled, all HTTP traffic between the browser and Cisco Secure ACS is encrypted, as reflected by the URLs, which begin with HTTPS. Additionally, most browsers include an indicator for when a connection is SSL-encrypted.

  To enable SSL, you must have completed the steps in Installing a Cisco Secure ACS Server Certificate, page 10-35, and Adding a Certificate Authority Certificate, page 10-37.



Downloaded from www.Manualslib.com manuals search engine

# Setting Up Access Policy

For information about access policy options, see Access Policy Options, page 12-12.

**Before You Begin**

If you want to enable SSL for administrative access, before completing this procedure, you must have completed the steps in Installing a Cisco Secure ACS Server Certificate, page 10-35, and Adding a Certificate Authority Certificate, page 10-37.

To set up Cisco Secure ACS Access Policy, follow these steps:

**Step 1** In the navigation bar, click **Administration Control**.

Cisco Secure ACS displays the Administration Control page.

**Step 2** Click **Access Policy**.

The Access Policy Setup page appears.

**Step 3** To allow remote access to the HTML interface from any IP address, in the IP Address Filtering table, select the **Allow all IP addresses to connect** option.

**Step 4** To allow remote access to the HTML interface only from IP addresses *within* a range or ranges of IP addresses, follow these steps:

**a.** In the IP Address Filtering table, select the **Allow only listed IP addresses to connect** option.

**b.** For each IP address range from within which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. In the Start IP Address box, type the lowest IP address (up to 16 characters) in the range. In the End IP Address box, type the highest IP address (up to 16 characters) in the range. Use dotted decimal format.

**Note** The IP addresses entered to define a range must differ only in the last octet.

**Step 5** To allow remote access to the HTML interface only from IP addresses *outside* a range or ranges of IP addresses, follow these steps:

**a.** In the IP Address Filtering table, select the **Reject connections from listed IP addresses** option.



Downloaded from www.Manualslib.com manuals search engine

b. For each IP address range from outside which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. Type the lowest IP address (up to 16 characters) in the range in the Start IP Address box. Type the highest IP address (up to 16 characters) in the range in the End IP Address box.

**Note** The IP addresses entered to define a range must differ only in the last octet.

**Step 6** If you want to allow Cisco Secure ACS to use any valid TCP port for administrative sessions, under HTTP Port Allocation, select the **Allow any TCP ports to be used for Administration HTTP Access** option.

**Step 7** If you want to allow Cisco Secure ACS to use only a specified range of TCP ports for administrative sessions, follow these steps:

a. Under HTTP Port Allocation, select the **Restrict Administration Sessions to the following port range From Port** *X* **to Port** *Y* option.

b. In the *X* box type the lowest TCP port (up to 5 characters) in the range.

c. In the *Y* box type the highest TCP port (up to 5 characters) in the range.

**Step 8** If you want to enable SSL encryption of administrator access to the HTML interface, under Secure Socket Layer Setup, select the **Use HTTPS Transport for Administration Access** check box.

**Note** To enable SSL, you must have completed the steps in Installing a Cisco Secure ACS Server Certificate, page 10-35, and Adding a Certificate Authority Certificate, page 10-37.

**Step 9** Click **Submit**.

Cisco Secure ACS saves and begins enforcing the access policy settings.

If you have enabled SSL, at the next administrator login, Cisco Secure ACS begins using HTTPS. Any current administrator sessions are unaffected.



Downloaded from www.Manualslib.com manuals search engine

# Session Policy

The Session Policy feature controls various aspects of Cisco Secure ACS administrative sessions.

This section contains the following topics:


- Session Policy Options, page 12-16
- Setting Up Session Policy, page 12-17


## Session Policy Options

You can configure the following options on the Session Policy Setup page:

- **Session idle timeout (minutes)**—Defines the time in minutes that an administrative session, local or remote, must remain idle before Cisco Secure ACS terminates the connection. This parameter applies to the Cisco Secure ACS administrative session in the browser only. It does not apply to an administrative dial-up session.

  An administrator whose administrative session is terminated receives a dialog box asking whether or not the administrator wants to continue. If the administrator chooses to continue, Cisco Secure ACS starts a new administrative session.

- **Allow Automatic Local Login**—Enables administrators to start an administrative session without logging in if they are using a browser on the computer running Cisco Secure ACS. Such administrative sessions are conducted using a default administrator account named “local_login”. The local_login administrator account has all privileges. Local administrative sessions with automatic local login are recorded in the Administrative Audit report under the local_login administrator name.

**Note** If there are no administrator accounts defined, no administrator name and password are required to access Cisco Secure ACS locally. This prevents you from accidentally locking yourself out of Cisco Secure ACS.



Downloaded from www.Manualslib.com manuals search engine

- **Respond to Invalid IP Address Connections**—Enables an error message in response to attempts to start a remote administrative session using an IP address that is invalid according to the IP address ranges configured in Access Policy. Disabling this option can help prevent unauthorized users from discovering Cisco Secure ACS.
- **Lock out Administrator after *X* successive failed attempts—**Enables Cisco Secure ACS to lock out an administrator after a number of successive failed attempts to log in to the HTML interface. The number of successive attempts is specified in the *X* box. If this check box is selected, the X box cannot be set to zero. If this check box is not selected, Cisco Secure ACS allows unlimited successive failed login attempts by an administrator.

# Setting Up Session Policy

For information about session policy options, see Session Policy Options, page 12-16.

To setup Cisco Secure ACS Session Policy, follow these steps:

**Step 1** In the navigation bar, click **Administration Control**.

Cisco Secure ACS displays the Administration Control page.

**Step 2** Click **Session Policy**.

The Session Policy Setup page appears.

**Step 3** To define the number of minutes of inactivity after which Cisco Secure ACS ends an administrative session, in the Session idle timeout (minutes) box, type the number of minutes (up to 4 characters).

**Step 4** Set the automatic local login policy:

**a.** To allow administrators to log in to Cisco Secure ACS locally without using their administrator names and passwords, select the **Allow Automatic Local Login** check box.

**b.** To require administrators to log in to Cisco Secure ACS locally using their administrator names and passwords, clear the **Allow Automatic Local Login** check box.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** Set the invalid IP address response policy:

a. To configure Cisco Secure ACS to respond with a message when an administrative session is requested from an invalid IP address, select the **Respond to invalid IP address connections** check box.

b. To configure Cisco Secure ACS to send no message when an administrative session is requested from an invalid IP address, clear the **Respond to invalid IP address connections** check box.

**Step 6** Set the failed administrative login attempts policy:

a. To enable Cisco Secure ACS to lock out an administrator after a specified number of successive failed administrative login attempts, select the **Lock out Administrator after** *X* **successive failed attempts** check box.

b. In the *X* box, type the number of successive failed login attempts after which Cisco Secure ACS locks out an administrator. The *X* box accepts up to 4 characters.

**Step 7** Click **Submit**.

Cisco Secure ACS saves and begins enforcing the session policy settings you made.

# Audit Policy

The Audit Policy feature controls the generation of the Administrative Audit log.

For more information about enabling, viewing, or configuring the Administrative Audit log, see Cisco Secure ACS System Logs, page 11-13.



Downloaded from www.Manualslib.com manuals search engine

# User Databases

Cisco Secure ACS for Windows Server authenticates users against one of several possible databases, including its internal database. You can configure Cisco Secure ACS to authenticate users with more than one type of database. This flexibility enables you to use user accounts data collected in different locations without having to explicitly import the users from each external user database into the CiscoSecure user database. It also enables you to apply different databases to different types of users, depending on the security requirements associated with user authorizations on your network. For example, a common configuration is to use a Windows user database for standard network users and a token server for network administrators.

**Note** For information about the Unknown User Policy and group mapping features, see Chapter 15, "Unknown User Policy" and Chapter 16, "User Group Mapping and Specification".

This chapter contains the following topics:


- CiscoSecure User Database, page 13-2
- About External User Databases, page 13-4
- Windows User Database, page 13-7
- Generic LDAP, page 13-32
- Novell NDS Database, page 13-49
- ODBC Database, page 13-55
- LEAP Proxy RADIUS Server Database, page 13-75




Downloaded from www.Manualslib.com manuals search engine

- Token Server User Databases, page 13-78
- Deleting an External User Database Configuration, page 13-86


# CiscoSecure User Database

The CiscoSecure user database is the database internal to Cisco Secure ACS. It supports authentication using ASCII, PAP, CHAP, MS-CHAP, ARAP, LEAP, EAP-MD5, EAP-TLS, PEAP(EAP-GTC), PEAP(EAP-MSCHAPv2), and EAP-FAST (phase zero and phase two).

The CiscoSecure user database is crucial for the authorization process. Regardless of whether a user is authenticated by the internal user database or by an external user database, Cisco Secure ACS authorizes network services for users based upon group membership and specific user settings found in the CiscoSecure user database. Thus, all users authenticated by Cisco Secure ACS, even those authenticated by an external user database, have an account in the CiscoSecure user database.

## About the CiscoSecure User Database

The CiscoSecure user database draws information from several data sources, including a memory-mapped, hash-indexed file, `VarsDB.MDB` (in Microsoft Jet database format), and the Windows Registry. `VarsDB.MDB` uses an index and tree structure, so searches can occur logarithmically rather than linearly, thus yielding very fast lookup times. This enables the CiscoSecure user database to authenticate users quickly.

For users authenticated using the CiscoSecure user database, Cisco Secure ACS stores user passwords in an encrypted format, using RC2 encryption with a 40-bit key. For users authenticated with external user databases, Cisco Secure ACS does not store passwords in the CiscoSecure user database.

Unless you have configured Cisco Secure ACS to authenticate users with an external user database, Cisco Secure ACS uses usernames and passwords in the CiscoSecure user database during authentication. For more information about specifying an external user database for authentication of a user, see Adding a Basic User Account, page 7-4.



Downloaded from www.Manualslib.com manuals search engine

# User Import and Creation

There are five ways to create user accounts in the in Cisco Secure ACS for Windows 2000 Servers. Of these, RDBMS Synchronization and CSUtil.exe support importing user accounts from external sources.

- **Cisco Secure ACS HTML interface**—The HTML interface provides the ability to create user accounts manually, one user at a time. Regardless of how a user account was created, you can edit a user account by using the HTML interface. For detailed steps, see Adding a Basic User Account, page 7-4.
- **Unknown User Policy**—The Unknown User Policy enables Cisco Secure ACS to add users automatically when a user without an account in the is found in an external user database. The creation of a user account in the occurs only when the user attempts to access the network and is successfully authenticated by an external user database. For more information, see Chapter 15, "Unknown User Policy".

  If you use Unknown User Policy, you can also configure group mappings so that each time a user added to the by Unknown User Policy is authenticated, the user group assignment is made dynamically. For some external user database types, user group assignment is based on group membership in the external user database. For other database types, all users authenticated by a given database are assigned to a single Cisco Secure ACS user group. For more information about group mapping, see Chapter 16, "User Group Mapping and Specification".
- **RDBMS Synchronization**—RDBMS Synchronization enables you to create large numbers of user accounts and to configure many settings for user accounts. We recommend using this feature whenever you need to import users by bulk; however, setting up RDBMS Synchronization for the first time requires several important decisions and time to implement them. For more information, see RDBMS Synchronization, page 9-25.
- **CSUtil.exe**—The CSUtil.exe command-line utility provides a simple means of creating basic user accounts. When compared to RDBMS Synchronization, its functionality is limited; however, it is simple to prepare for importing basic user accounts and assigning users to groups. For more information, see Appendix D, "CSUtil Database Utility".
- **Database Replication**—Database Replication creates user accounts on a secondary Cisco Secure ACS by overwriting all existing user accounts on a secondary Cisco Secure ACS with the user accounts from the primary



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS. Any user accounts unique to a secondary Cisco Secure ACS are lost in the replication. For more information, see CiscoSecure Database Replication, page 9-1.

# About External User Databases

You can configure Cisco Secure ACS to forward authentication of users to one external user database or more. Support for external user databases means that Cisco Secure ACS does not require that you create duplicate user entries in the CiscoSecure user database. In organizations in which a substantial user database already exists, Cisco Secure ACS can leverage the work already invested in building the database without any additional input.

In addition to performing authentication for network access, Cisco Secure ACS can perform authentication for TACACS+ enable privileges using external user databases. For more information about TACACS+ enable passwords, see Setting TACACS+ Enable Password Options for a User, page 7-35.

**Note** You can only use external users databases to authenticate users and to determine which group Cisco Secure ACS assigns a user to. The CiscoSecure user database, internal to Cisco Secure ACS, provides all authorization services. With few exceptions, Cisco Secure ACS cannot retrieve authorization data from external user databases. Exceptions are noted where applicable in the discussions of specific databases in this chapter. For more information about group mapping for unknown users, see Chapter 16, "User Group Mapping and Specification".

Users can be authenticated using the following databases:

- Windows Database
- Generic LDAP
- Novell NetWare Directory Services (NDS)
- Open Database Connectivity (ODBC)-compliant relational databases
- LEAP Proxy RADIUS servers
- RSA SecurID token servers
- RADIUS-compliant token servers



Downloaded from www.Manualslib.com manuals search engine

For Cisco Secure ACS to interact with an external user database, Cisco Secure ACS requires an API for third-party authentication source. The Cisco Secure ACS communicates with the external user database using the API. For Windows user databases and Generic LDAP, the program interface for the external authentication is local to Cisco Secure ACS. In these cases, no further components are required.

In the case of Novell NDS authentication, Novell Requestor must be installed on the same Windows server as Cisco Secure ACS.

In the case of ODBC authentication sources, in addition to the Windows ODBC interface, the third-party ODBC driver must be installed on the Cisco Secure ACS Windows server.

To communicate with an RSA token server, you must have installed software components provided by RSA. For token servers by other vendors, the standard RADIUS interface serves as the third-party API.

# Authenticating with External User Databases

Authenticating users with an external user database requires more than configuring Cisco Secure ACS to communicate with an external user database. Performing one of the configuration procedures for an external database that are provided in this chapter does not on its own instruct Cisco Secure ACS to authenticate any users with that database.

After you have configured Cisco Secure ACS to communicate with an external user database, you can configure Cisco Secure ACS to authenticate users with the external user database in one of two ways:

- **By Specific User Assignment**—You can configure Cisco Secure ACS to authenticate specific users with an external user database. To do this, the user must exist in the CiscoSecure user database and the Password Authentication list in User Setup must be set to the external user database that Cisco Secure ACS should use to authenticate the user.

  While setting the Password Authentication for every user account is time consuming, this method of determining which users are authenticated with an external user database is secure because it requires explicit definition of who should authenticate using the external user database. In addition, the users may be placed in the desired Cisco Secure ACS group and thereby receive the applicable access profile.



Downloaded from www.Manualslib.com manuals search engine

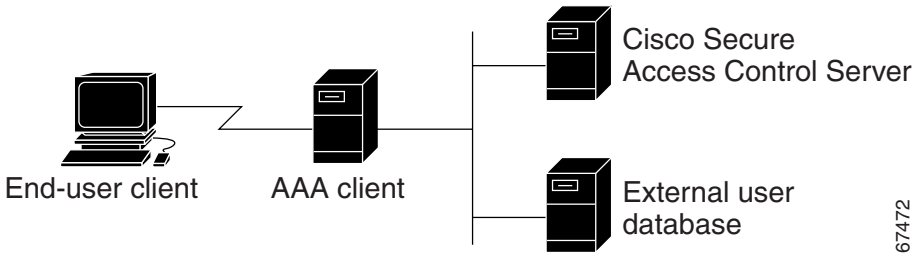
- **By Unknown User Policy**—You can configure Cisco Secure ACS to attempt authentication of users not found in the CiscoSecure user database by using an external user database. Users do not need to be defined in the CiscoSecure user database for this method. For more information about the Unknown User Policy, see About Unknown User Authentication, page 15-4.

You can also configure Cisco Secure ACS with both methods above; these two methods are not mutually exclusive.

# External User Database Authentication Process

When Cisco Secure ACS attempts user authentication with an external user database, it forwards the user credentials to the external user database. The external user database either passes or fails the authentication request from Cisco Secure ACS. Upon receiving the response from the external user database, Cisco Secure ACS instructs the requesting AAA client to grant or deny the user access, depending upon the response from the external user database. Figure 13-1 shows a AAA configuration with an external user database.

***Figure 13-1 A Simple AAA Scenario***




The specifics of the method used to communicate with the external user database vary with the database type. For LDAP and Novell NDS, Cisco Secure ACS uses TCP connections. For Windows user databases, Cisco Secure ACS uses the authentication API provided in the Windows operating system. With the exception of RSA token servers, Cisco Secure ACS communicates with token servers using RADIUS. For RSA token servers, Cisco Secure ACS acts an RSA client in order to use the RSA proprietary interface.

For more information, see the section regarding the database type you are interested in.



Downloaded from www.Manualslib.com manuals search engine

# Windows User Database

You can configure Cisco Secure ACS to use a Windows user database to authenticate users.

This section contains the following topics:


- What's Supported with Windows User Databases, page 13-8
- Authentication with Windows User Databases, page 13-9
- Trust Relationships, page 13-9
- Windows Dial-up Networking Clients, page 13-10
  - Windows Dial-up Networking Clients with a Domain Field, page 13-10
  - Windows Dial-up Networking Clients without a Domain Field, page 13-11
- Usernames and Windows Authentication, page 13-11
  - Username Formats and Windows Authentication, page 13-11
  - Non-domain-qualified Usernames, page 13-13
  - Domain-Qualified Usernames, page 13-14
  - UPN Usernames, page 13-14
- EAP and Windows Authentication, page 13-15
  - EAP-TLS Domain Stripping, page 13-16
  - Machine Authentication, page 13-16
  - Machine Access Restrictions, page 13-19
  - Microsoft Windows and Machine Authentication, page 13-20
  - Enabling Machine Authentication, page 13-22
- User-Changeable Passwords with Windows User Databases, page 13-25
- Preparing Users for Authenticating with Windows, page 13-26
- Windows User Database Configuration Options, page 13-26
- Configuring a Windows External User Database, page 13-30




Downloaded from www.Manualslib.com manuals search engine

# What's Supported with Windows User Databases

Cisco Secure ACS supports the use of Windows external user databases for the following features:

- **User Authentication**—Cisco Secure ACS supports ASCII, PAP, MS-CHAP (versions 1 and 2), LEAP, PEAP(EAP-GTC), PEAP(EAP-MSCHAPv2), and EAP-FAST (phase zero and phase two) authentication with Windows Security Accounts Manager (SAM) database or a Windows Active Directory database. Cisco Secure ACS also supports EAP-TLS authentication with a Windows Active Directory database. Other authentication protocols are not supported with Windows external user databases.

  **Note** Authentication protocols not supported with Windows external user databases may be supported by a different external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-10.

- **Machine Authentication**—Cisco Secure ACS supports machine authentication with EAP-TLS and PEAP(EAP-MSCHAPv2). For more information, see EAP and Windows Authentication, page 13-15.
- **Group Mapping for Unknown Users**—Cisco Secure ACS supports group mapping for unknown users by requesting group membership information from Windows user databases. For more information about group mapping for users authenticated with a Windows user database, see Group Mapping by Group Set Membership, page 16-4.
- **Password-Aging**—Cisco Secure ACS supports password aging for users authenticated by a Windows user database. For more information, see User-Changeable Passwords with Windows User Databases, page 13-25.
- **Dial-in Permissions**—Cisco Secure ACS supports use of dial-in permissions from Windows user databases. For more information, see Preparing Users for Authenticating with Windows, page 13-26.
- **Callback Settings**—Cisco Secure ACS supports use of callback settings from Windows user databases. For information about configuring Cisco Secure ACS to use Windows callback settings, see Setting User Callback Option, page 7-9.



Downloaded from www.Manualslib.com manuals search engine

# Authentication with Windows User Databases

Cisco Secure ACS forwards user credentials to a Windows database by passing the user credentials to the Windows operating system of the computer running Cisco Secure ACS. The Windows database either passes or fails the authentication request from Cisco Secure ACS. Upon receiving the response from the Windows database, Cisco Secure ACS instructs the requesting AAA client to grant or deny the user access, depending upon the response from the Windows database.

Cisco Secure ACS grants authorization based on the Cisco Secure ACS group to which the user is assigned. While the group to which a user is assigned can be determined by information from the Windows database, it is Cisco Secure ACS that grants authorization privileges.

To further control access by a user, you can configure Cisco Secure ACS to also check the setting for granting dialin permission to the user. This setting is labeled "Grant dialin permission to user" in Windows NT and "Allow access" in the Remote Access Permission area in Windows 2000. If this feature is disabled for the user, access is denied, even if the username and password are typed correctly.

# Trust Relationships

Cisco Secure ACS can take advantage of trust relationships that have been established between Windows domains. If the domain that contains Cisco Secure ACS trusts another domain, Cisco Secure ACS can authenticate users whose accounts reside in the other domain. Cisco Secure ACS can also reference the "Grant dialin permission to user" setting across trusted domains.

**Note** If Cisco Secure ACS is running on a member server rather than a domain controller, taking advantage of trust relationships depends upon proper configuration of Cisco Secure ACS at installation. For more information, see "Windows Authentication from a Member Server" in *Installation Guide for Cisco Secure ACS for Windows Server.*

Cisco Secure ACS can take advantage of indirect trusts for Windows authentication. Consider the example of Windows domains A, B, and C, where Cisco Secure ACS resides on a server in domain A. Domain A trusts domain B,



Downloaded from www.Manualslib.com manuals search engine

but no trust relationship is established between domain A and domain C. If domain B trusts domain C, Cisco Secure ACS in domain A can authenticate users whose accounts reside in domain C, making use of the indirect trust of domain C.

For more information on trust relationships, refer to your Microsoft Windows documentation.

# Windows Dial-up Networking Clients

The dial-up networking clients for Windows NT/2000/XP Professional and Windows 95/98/Millennium Edition (ME)/XP Home enable users to connect to your network remotely, but the fields provided differ.

## Windows Dial-up Networking Clients with a Domain Field

If users dial in to your network using the dial-up networking client provided with Windows NT, Windows 2000, or Windows XP Professional, three fields appear:

- **username**—Type your username.
- **password**—Type your password.
- **domain**—Type your valid domain name.

**Note** For more information about the implications of completing or leaving the domain box blank, see Non-domain-qualified Usernames, page 13-13.



Downloaded from www.Manualslib.com manuals search engine

## Windows Dial-up Networking Clients without a Domain Field

If users access your network using the dial-up networking client provided with Windows 95, Windows 98, Windows ME, or Windows XP Home, two fields appear:

- **username**—Type your username.

  **Note** You can also prefix your username with the name of the domain you want to log in to. For more information about the implications of prefixing or not prefixing the domain name before the username, see Non-domain-qualified Usernames, page 13-13.

- **password**—Type your password.

# Usernames and Windows Authentication

This section contains the following topics:


- Username Formats and Windows Authentication, page 13-11
- Non-domain-qualified Usernames, page 13-13
- Domain-Qualified Usernames, page 13-14
- UPN Usernames, page 13-14


## Username Formats and Windows Authentication

Cisco Secure ACS supports Windows authentication for usernames in a variety of formats. When Cisco Secure ACS attempts Windows authentication, it first determines the username format and submits the username to Windows in the applicable manner. To implement reliable Windows authentication with Cisco Secure ACS, you need to understand how Cisco Secure ACS determines username format, how it supports for each of these formats, and how the types of support are related.



Downloaded from www.Manualslib.com manuals search engine

To determine the format of a username submitted for Windows authentication, Cisco Secure ACS searches the username for the presence of the following two special characters:

- @ (the "at" character)
- \ (the "backslash" character)

Based upon the presence and position of these two characters in the username, Cisco Secure ACS determines username format as follows:

1. If the username does not contain a "backslash" character *and* does not contain an "at" character, Cisco Secure ACS considers the username to be non-domain qualified. For example, the username `cyril.yang` is non-domain qualified. For more information, see Non-domain-qualified Usernames, page 13-13.
2. If the username contains a "backslash" character that precedes any "at" characters, Cisco Secure ACS considers the username to be domain qualified. For example, Cisco Secure ACS considers the following usernames to be domain qualified:
   - MAIN\cyril.yang
   - MAIN\cyril.yang@central-office

   For more information, see Domain-Qualified Usernames, page 13-14.
3. If the username contains an "at" character that is not preceded by a "backslash" character, Cisco Secure ACS considers the username to be in UPN format. For example, Cisco Secure ACS considers the following usernames to be UPN usernames:
   - cyril.yang@example.com
   - cyril.yang@main.example.com
   - cyril.yang@main
   - cyril.yang@central-office@example.com
   - cyril.yang@main\example.com

   For more information, see UPN Usernames, page 13-14.



Downloaded from www.Manualslib.com manuals search engine

## Non-domain-qualified Usernames

Cisco Secure ACS supports Windows authentication of usernames that are not domain qualified, provided the username does not contain an "at" character. Users with "at" characters in their usernames must either submit the username in UPN format or in a domain-qualified format. Examples of non-domain-qualified usernames are cyril.yang and msmith.

In Windows environments with multiple domains, authentication results with non-domain-qualified usernames can vary. This is because Windows, not Cisco Secure ACS, determines which domains are used to authenticate a non-domain-qualified username. If Windows does not find the username in its local domain database, it then checks all trusted domains. If Cisco Secure ACS runs on a member server and the username is not found in trusted domains, Windows also checks its local accounts database. Windows attempts to authenticate a user with the first occurrence of the username that it finds.

When Windows authentication for a non-domain-qualified username succeeds, the privileges assigned upon authentication will be those associated with the Windows user account in the first domain with a matching username and password. This also illustrates the importance of removing usernames from a domain when the user account is no longer needed.

**Note** If the credentials submitted by the user do not match the credentials associated with the first matching username that Windows finds, authentication fails. Thus, if different users in different domains share the same exact username, logging in with a non-domain-qualified username can result in inadvertent authentication failure.

Use of the Domain List is not required to support Windows authentication, but it can alleviate authentication failures caused by non-domain-qualified usernames. If you have configured the Domain List in the Windows User Database Configuration page of the External User Databases section, Cisco Secure ACS submits the username and password to each domain in the list in a domain-qualified format until it successfully authenticates the user. If Cisco Secure ACS has tried each domain listed in the Domain List or if no trusted domains have been configured in the Domain List, Cisco Secure ACS stops attempting to authenticate the user and does not grant that user access.



Downloaded from www.Manualslib.com manuals search engine

**Note** If your Domain List contains domains and your Windows SAM or Active Directory user databases are configured to lock out users after a number of failed attempts, users can be inadvertently locked out because Cisco Secure ACS tries each domain in the Domain List explicitly, resulting in failed attempts for identical usernames that reside in different domains.

## Domain-Qualified Usernames

The most reliable method of authenticating users against a specific domain is to require users to submit the domains they should be authenticated against along with their usernames. Authentication of a domain-qualified username is directed to a specific domain rather than depending upon Windows to attempt authentication with the correct domain or upon using the Domain List to direct Cisco Secure ACS to submit the username repeatedly in a domain-qualified format.

Domain-qualified usernames have the following format:

*DOMAIN\user*

For example, the domain-qualified username for user Mary Smith (msmith) in Domain10 would be Domain10\msmith.

For usernames containing an "at" character, such as cyril.yang@central-office, using a domain-qualified username format is required. For example, MAIN\cyril.yang@central-office. If a username containing an "at" character is received in a non-domain-qualified format, Cisco Secure ACS perceives it as a username in UPN format. For more information, see UPN Usernames, page 13-14.

## UPN Usernames

Cisco Secure ACS supports authentication of usernames in User Principal Name (UPN) format, such as cyril.yang@example.com or cyril.yang@central-office@example.com.



Downloaded from www.Manualslib.com manuals search engine

If the authentication protocol used is EAP-TLS, by default, Cisco Secure ACS submits the username to Windows in UPN format; however, you can configure Cisco Secure ACS to strip from the username all characters after and including the last "at" character (@). For more information, see EAP-TLS Domain Stripping, page 13-16.

For all other authentication protocols that it can support with Windows databases, Cisco Secure ACS submits to Windows the username stripped of all characters after and including the last "at" character (@). This behavior allows for usernames that contain an "at" character. For example:

- If the username received is cyril.yang@example.com, Cisco Secure ACS submits to Windows an authentication request containing the username cyril.yang.
- If the username received is cyril.yang@central-office@example.com, Cisco Secure ACS submits to Windows an authentication request containing the username cyril.yang@central-office.

**Note** Cisco Secure ACS cannot tell the difference between a non-domain-qualified username that contains an "at" character and a UPN username; all usernames containing an "at" character that are not preceded by a "backslash" character are submitted to Windows with the final "at" character and the characters that follow it removed. Users with "at" characters in their usernames must either submit the username in UPN format or in a domain-qualified format.

# EAP and Windows Authentication

This section provides information about Windows-specific EAP features that you can configure on the Windows User Database Configuration page.

This section contains the following topics:

- EAP-TLS Domain Stripping, page 13-16
- Machine Authentication, page 13-16
- Machine Access Restrictions, page 13-19
- Microsoft Windows and Machine Authentication, page 13-20
- Enabling Machine Authentication, page 13-22



Downloaded from www.Manualslib.com manuals search engine

## EAP-TLS Domain Stripping

If you use Windows Active Directory to authenticate users with EAP-TLS, Cisco Secure ACS enables you to strip the domain name from the username stored in the Subject Alternative Name field of the user certificate. Performing domain name stripping can speed EAP-TLS authentication when the domain that must authenticate a user is not the domain represented in the SAN field.

For example, a user's SAN field may contain "jsmith@corporation.com" but jsmith may need to authenticate using the domain controller for a subdomain named "engineering". Stripping "@corporation.com" from the username eliminates the needless attempt at authenticating jsmith against the corporation.com domain controller. Without stripping the domain name, only after jsmith cannot be found in corporation.com will Cisco Secure ACS use the Domain List and find the user in the engineering domain. The additional delay could be several seconds. For more information about the Domain List, see Non-domain-qualified Usernames, page 13-13.

You can enable EAP-TLS domain name stripping on the Windows User Database Configuration page.

**Note** EAP-TLS domain name stripping operates independently of support for UPN-formatted usernames. For information about support for Windows authentication of UPN-formatted usernames, see UPN Usernames, page 13-14.

## Machine Authentication

Cisco Secure ACS supports the authentication of computers running Microsoft Windows operating systems that support EAP computer authentication, such as Windows XP with Service Pack 1. Machine authentication, also called computer authentication, allows networks services only for computers known to Active Directory. This is especially useful for wireless networks, where unauthorized users outside the physical premises of your workplace can access your wireless access points.



Downloaded from www.Manualslib.com manuals search engine

When machine authentication is enabled, there are three different types of authentications. Upon starting up a computer, the authentications occur in the following order:

- **Machine authentication**—The computer is authenticated by Cisco Secure ACS prior to user authentication. Cisco Secure ACS checks the credentials provided by the computer against the Windows user database. If you use Active Directory and the matching computer account in Active Directory has the same credentials, the computer gains access to Windows domain services.
- **User domain authentication**—If machine authentication succeeded, the user is authenticated by the Windows domain. If machine authentication failed, the computer does not have access to Windows domain services and the user credentials are authenticated using cached credentials kept by the local operating system. When a user is authenticated by cached credentials instead of the domain, the computer does not enforce domain policies, such as running login scripts dictated by the domain.

**Tip** If a computer fails machine authentication and the user hasn't successfully logged in to the domain using the computer since the most recent user password change, the cached credentials on the computer will not match the new password. Instead, the cached credentials will match an older password of the user, provided that the user once logged in to the domain successfully from this computer.

- **User network authentication**—The user is authenticated by Cisco Secure ACS, allowing the user to have network connectivity. If the user profile exists, the user database specified is used to authenticate the user. While the user database is not required to be the Windows user database, most Microsoft clients can be configured to automatically perform network authentication using the same credentials used for user domain authentication. This allows for a single sign-on.

**Note** Microsoft PEAP clients also initiate machine authentication whenever a user logs off. This prepares the network connection for the next user login. Microsoft PEAP clients may also initiate machine authentication when a user has selected to shutdown or restart the computer rather than just logging off.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS supports both EAP-TLS and PEAP(EAP-MSCHAPv2) for machine authentication. You can enable each separately on the Windows User Database Configuration page, which allows a mix of computers authenticating with EAP-TLS or with PEAP(EAP-MSCHAPv2). Microsoft operating systems that perform machine authentication may limit the user authentication protocol to the same protocol used for machine authentication. For more information about Microsoft operating systems and machine authentication, see Microsoft Windows and Machine Authentication, page 13-20.

The Unknown User Policy supports machine authentication. Computers previously unknown to Cisco Secure ACS are handled similarly to users. If the Unknown User Policy is enabled and an Active Directory external user database is included on the Selected Databases list on the Configure Unknown User Policy page, machine authentication succeeds, provided that the machine credentials presented to Active Directory are valid.

On a computer configured to perform machine authentication, machine authentication occurs when the computer started. Provided that the AAA client sends RADIUS accounting data to Cisco Secure ACS, when a computer is started and before a user logs in on that computer, the computer appears on the Logged-In Users List in the Reports and Activity section. Once user authentication begins, the computer no longer appears on the Logged-In Users List.

PEAP-based machine authentication uses PEAP(EAP-MSCHAPv2) and the password for the computer established automatically when it was added to the Microsoft Windows domain. The computer sends its name as the username and the format is:

`host/`*computer*`.`*domain*

where *computer* is the name of the computer and *domain* is the domain the computer belongs to. The domain segment may include subdomains, too, if they are used, so that the format may be:

`host/`*computer*`.`*subdomain*`.`*domain*

The usernames of computers authenticated must appear in the CiscoSecure user database. If you enable unknown user processing, Cisco Secure ACS adds them automatically once they authenticate successfully. During authentication, the domain name is not used.

EAP-TLS-based machine authentication uses EAP-TLS to authenticate the computer using a client certificate. The certificate used by the computer can be one installed automatically when the computer was added to the domain or one



Downloaded from www.Manualslib.com manuals search engine

that was added to the local machine storage later. As with PEAP-based machine authentication, the computer name must appear in the CiscoSecure user database in the format contained in the computer client certificate and the user profile corresponding to the computer name must be configured to authenticate using the Windows external user database. If you enable unknown user processing, Cisco Secure ACS adds the computer names to the CiscoSecure user database automatically once they authenticate successfully. It also automatically configures the user profiles created to use the external user database that the user was found in. For machine authentication, this will always be the Windows external user database.

## Machine Access Restrictions

You can use the machine access restrictions (MAR) feature as an additional means of controlling authorization for Windows-authenticated EAP-TLS and Microsoft PEAP users, based upon machine authentication of the computer used to access the network. When you enable the MAR feature, Cisco Secure ACS does the following:

- For every successful machine authentication, Cisco Secure ACS caches the value received in IETF RADIUS Calling-Station-Id attribute (31) as evidence of the successful machine authentication. Cisco Secure ACS stores each Calling-Station-Id attribute value for the number of hours specified on the Windows User Database Configuration page before deleting it from the cache.
- When a user authenticates with an EAP-TLS or Microsoft PEAP end-user client, Cisco Secure ACS searches the cache of Calling-Station-Id values from successful machine authentications for the Calling-Station-Id value received in the user authentication request. Whether Cisco Secure ACS finds the user-authentication Calling-Station-Id value in the cache affects how Cisco Secure ACS assigns the user requesting authentication to a user group.
  - **Calling-Station-Id value found in the cache**—Cisco Secure ACS assigns the user to a user group by normal methods, which include manual specification of a group in the user profile, group mapping, or RADIUS-based group specification. For example, if a user logs in with a computer that was successfully authenticated and the user profile indicates that the user is a member of group 137, Cisco Secure ACS applies to the user session the authorization settings specified in group 137.



Downloaded from www.Manualslib.com manuals search engine

– **Calling-Station-Id value not found in the cache**—Cisco Secure ACS assigns the user to the user group specified by "Group map for successful user authentication without machine authentication" list. This can include the <No Access> group.

**Note** User profile settings always override group profile settings. If a user profile grants an authorization that is denied by the group specified in the "Group map for successful user authentication without machine authentication" list, Cisco Secure ACS grants the authorization.

The MAR feature supports full EAP-TLS and Microsoft PEAP authentication, as well as resumed sessions for EAP-TLS and Microsoft PEAP and fast reconnections for Microsoft PEAP.

The MAR feature has the following limitations and requirements:

- Machine authentication must be enabled.
- Users must authenticate with EAP-TLS or a Microsoft PEAP client. MAR does not apply to users authenticated by other protocols, such as EAP-FAST, LEAP, or MS-CHAP.
- The AAA client must send a value in the IETF RADIUS Calling-Station-Id attribute (31).
- Cisco Secure ACS does not replicate the cache of Calling-Station-Id attribute values from successful machine authentications.

## Microsoft Windows and Machine Authentication

Cisco Secure ACS supports machine authentication with Active Directory in Windows 2000. To enable machine authentication support in Windows 2000 Active Directory you must:

- Apply Service Pack 4 to the computer running Active Directory.
- Complete the steps in Microsoft Knowledge Base Article 306260: Cannot Modify Dial-In Permissions for Computers That Use Wireless Networking.



Downloaded from www.Manualslib.com manuals search engine

Client operating systems supporting machine authentication are:

- Microsoft Windows XP with Service Pack 1 applied.
- Microsoft Windows 2000 with the following:
  - Service Pack 4 applied.
  - Patch Q313664 applied (available from Microsoft.com).

The following list describes the essential details of enabling machine authentication on a client computer with a Cisco Aironet 350 wireless adapter. For more information about enabling machine authentication in Microsoft Windows operating systems, please refer to Microsoft documentation.

1. Make sure the wireless network adapter is installed correctly. For more information, see the documentation provided with the wireless network adapter.
2. Make sure the certification authority (CA) certificate of the CA that issued the Cisco Secure ACS server certificate is stored in machine storage on client computers. User storage is not available during machine authentication; therefore, if the CA certificate is in user storage, machine authentication fails.
3. Select the wireless network:
   - In Windows XP, you can select the network on the Wireless Networks tab of the wireless network connection properties.
   - In Windows 2000, you can enter the SSID of the wireless network manually. This is done on the Advanced tab of the properties dialog box for the wireless network adapter.
4. To enable PEAP machine authentication, configure the Authentication tab. In Windows XP, the Authentication tab is available from the properties of the wireless network. In Windows 2000, it is available from the properties of the wireless network connection.
   a. Select the **Enable network access control using IEEE 802.1X** check box.
   b. Select the **Authenticate as computer when computer information is available** check box.
   c. From the **EAP type** list, select **Protected EAP (PEAP)**.



Downloaded from www.Manualslib.com manuals search engine

d. On the Protected EAP Properties dialog box, you can enforce that Cisco Secure ACS has a valid server certificate by selecting the **Validate server certificate** check box. If you do select this check box, you must also select the applicable Trusted Root Certification Authorities.

e. Also open the PEAP properties dialog box, from the **Select Authentication Method** list, select **Secured password (EAP-MSCHAP v2)**.

5. To enable EAP-TLS machine authentication, configure the Authentication tab. In Windows XP, the Authentication tab is available from the properties of the wireless network. In Windows 2000, it is available from the properties of the wireless network connection.

   a. Select the **Enable network access control using IEEE 802.1X** check box.

   b. Select the **Authenticate as computer when computer information is available** check box.

   c. From the **EAP type** list, select **Smart Card or other Certificate**.

   d. On the Smart Card or other Certificate Properties dialog box, select the **Use a certificate on this computer** option.

   e. Also on the Smart Card or other Certificate Properties dialog box, you can enforce that Cisco Secure ACS has a valid server certificate by selecting the **Validate server certificate** check box. If you do select this check box, you must also select the applicable Trusted Root Certification Authorities.

If you have a Microsoft certification authority server configured on the domain controller, you can configure a policy in Active Directory to produce a client certificate automatically when a computer is added to the domain. For more information, see Microsoft Knowledge Base Article 313407, HOW TO: Create Automatic Certificate Requests with Group Policy in Windows.

## Enabling Machine Authentication

This procedure provides an overview of the detailed procedures required to configure Cisco Secure ACS to support machine authentication.



Downloaded from www.Manualslib.com manuals search engine

**Note** End-user client computers and the applicable Active Directory must be configured to support machine authentication. This procedure is specific to configuration of Cisco Secure ACS only. For information about configuring Microsoft Windows operating systems to support machine authentication, see Microsoft Windows and Machine Authentication, page 13-20.

To enable Cisco Secure ACS to perform machine authentication, follow these steps:

**Step 1** Install a server certificate in Cisco Secure ACS. PEAP(EAP-MSCHAPv2) and EAP-TLS require a server certificate. Cisco Secure ACS uses a single certificate to support both protocols. For detailed steps, see Installing a Cisco Secure ACS Server Certificate, page 10-35.

**Note** If you have installed a certificate to support EAP-TLS or PEAP user authentication or to support HTTPS protection of remote Cisco Secure ACS administration, you do not need to perform this step. A single server certificate will support all certificate-based Cisco Secure ACS services and remote administration.

**Step 2** For EAP-TLS machine authentication, if certificates on end-user clients are issued by a different CA than the CA that issued the server certificate on Cisco Secure ACS, you must edit the certification trust list so that CAs issuing end-user client certificates are trusted. If you do not perform this step and the CA of the server certificate is not the same as the CA of an end-user client certificate CA, EAP-TLS will operate normally but reject the EAP-TLS machine authentication because it does not trust the correct CA. For detailed steps, see Editing the Certificate Trust List, page 10-38.

**Step 3** Enable the applicable protocols on the Global Authentication Setup page:

- To support machine authentication with PEAP, enable the PEAP(EAP-MSCHAPv2) protocol.
- To support machine authentication with EAP-TLS, enable the EAP-TLS protocol.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS allows you to complete this step only after you have successfully completed Step 1. For detailed steps, see Configuring Authentication Options, page 10-33.

**Step 4** Configure a Windows external user database and enable the applicable types of machine authentication on the Windows User Database Configuration page:

- To support machine authentication with PEAP, select the **Permit PEAP machine authentication** check box.
- To support machine authentication with EAP-TLS, select the **Permit EAP-TLS machine authentication** check box.
- To require machine authentication in addition to user authentication, select the **Enable machine access restrictions** check box.

**Note** If you already have a Windows external user database configured, modify its configuration to enable the applicable machine authentication types.

For detailed steps, see Configuring a Windows External User Database, page 13-30.

Cisco Secure ACS is ready to perform machine authentication for computers whose names exist in CiscoSecure user database.

**Step 5** If you have not already enabled the Unknown User Policy and added the Windows external user database to the Selected Databases list, consider doing so to allow computers that are not known to Cisco Secure ACS to authenticate. For detailed steps, see Configuring the Unknown User Policy, page 15-16.

**Note** Enabling the Unknown User Policy to support machine authentication also enables the Unknown User Policy for user authentication. Cisco Secure ACS makes no distinction in unknown user support between computers and users.

Cisco Secure ACS is ready to perform machine authentication for computers, regardless of whether the computer names exist in CiscoSecure user database.



Downloaded from www.Manualslib.com manuals search engine

# User-Changeable Passwords with Windows User Databases

For network users who are authenticated by a Windows user database, Cisco Secure ACS supports user-changeable passwords upon password expiration. You can enable this feature in the MS-CHAP Settings and Windows EAP Settings tables on the Windows User Database Configuration page in the External User Databases section. Using this feature in your network requires the following:

- Users must be present in the Windows Active Directory or SAM user database.
- User accounts in Cisco Secure ACS must specify the Windows user database for authentication.
- End-user clients must be compatible with MS-CHAP, PEAP(EAP-GTC), PEAP(EAP-MSCHAPv2), or EAP-FAST.
- The AAA client that the end-user clients connect to must support the applicable protocols:
  - For MS-CHAP password aging, the AAA client must support RADIUS-based MS-CHAP authentication.
  - For PEAP(EAP-MSCHAPv2), PEAP(EAP-GTC), and EAP-FAST password aging, the AAA client must support EAP.

When the conditions above are met and this feature is enabled, users receive a dialog box prompting them to change their passwords upon their first successful authentication after their passwords have expired. The dialog box is the same as presented to users by Windows when a user with an expired password accesses a network via a remote access server.

For more information about password aging support in Cisco Secure ACS, see Enabling Password Aging for Users in Windows Databases, page 6-26.



Downloaded from www.Manualslib.com manuals search engine

# Preparing Users for Authenticating with Windows

Before using the Windows user database for authentication, follow these steps:

**Step 1** Make sure the username exists in the Windows user database.

**Step 2** In Windows, for each user account, clear the following User Properties check boxes:

- User must change password at next logon
- Account disabled

**Step 3** If you want to control dial-in access from within Windows NT, click **Dial-in** and select **Grant dialin permission to user**. In Windows 2000, access the User Properties dialog box, select the **Dial-In** tab, and in the Remote Access area, click **Allow access**. You must also configure the option to reference this feature under Database Group Mappings in the External User Databases section of Cisco Secure ACS.

# Windows User Database Configuration Options

The Windows User Database Configuration page contains the following configuration options:

- **Dialin Permission**—You can restrict network access to users whose Windows accounts have Windows dialin permission. The Grant dialin permission to user check box controls this feature.

**Note** This feature applies to all users authenticated by Cisco Secure ACS with a Windows external user database; despite the name of the feature, it is not limited to users who access the network with a dialup client but is applied regardless of client type. For example, if you have configured a PIX Firewall to authenticate Telnet sessions using Cisco Secure ACS as a RADIUS server, a user authenticated by a Windows external user database would be denied Telnet access to the PIX Firewall if the Dialin Permission feature is enabled and the Windows user account does not have dialin permission.



Downloaded from www.Manualslib.com manuals search engine

**Tip** Windows dialin permission is enabled in the Dialin section of user properties in Windows NT and on the Dial-In tab of the user properties in Windows 2000.

- **Configure Domain List**—The Domain List controls what Cisco Secure ACS does when user authentication is requested for a username that is not domain-qualified. If no domains are in the Domain List and the initial user authentication request is rejected by Windows, Cisco Secure ACS stops attempting to authenticate the user. If domains are in the Domain List, Cisco Secure ACS qualifies the username with a domain from the list and submits the domain-qualified username to Windows, once for each domain in the Domain List, until each domain has rejected the user or until one of the domains authenticates the user.

  **Note** Configuring the Domain List list is optional. For more information about the Domain List, see Non-domain-qualified Usernames, page 13-13.

**Caution** If your Domain List contains domains and your Windows SAM or Active Directory user databases are configured to lock out users after a number of failed attempts, users can be inadvertently locked out because Cisco Secure ACS tries each domain in the Domain List explicitly, resulting in failed attempts for identical usernames that reside in different domains.

  - **Available Domains**—This list represents the domains that Cisco Secure ACS *does not* send domain-qualified authentication requests to.
  - **Domain List**—This list represents the domains that Cisco Secure ACS *does* send domain-qualified authentication requests to.

- **MS CHAP Settings**—You can control whether Cisco Secure ACS supports MS-CHAP-based password changes for Windows user accounts. The Permit password changes using MS-CHAP version *N* check boxes enable you to specify which versions of MS CHAP Cisco Secure ACS supports password changes using.



Downloaded from www.Manualslib.com manuals search engine

**Note** The check boxes under MS CHAP Settings do no affect password aging for Microsoft PEAP, EAP-FAST, or machine authentication.

For more information about Windows password changes, see Enabling Password Aging for Users in Windows Databases, page 6-26.

- **Enable password change inside PEAP or EAP-FAST**—The Permit password change inside PEAP or EAP-FAST check box controls whether Cisco Secure ACS supports PEAP-based or EAP-FAST-based password changes for Windows user accounts. PEAP password changes are supported only when the end-user client uses PEAP(EAP-MSCHAPv2) for user authentication. For EAP-FAST, Cisco Secure ACS supports password changes in phase zero and phase two.
- **EAP-TLS Strip Domain Name**—The EAP-TLS Strip Domain Name check box controls whether Cisco Secure ACS removes the domain name from a username derived from the Subject Alternative Name (SAN) field in an end-user certificate.

  Performing domain name stripping can speed EAP-TLS authentication when the domain that must authenticate a user is not the domain represented in the SAN field. For example, a user's SAN field may contain "jsmith@corporation.com" but jsmith may need to authenticate using the domain controller for a subdomain named "engineering". Stripping "@corporation.com" from the username eliminates the needless attempt at authenticating jsmith against the corporation.com domain controller. Without stripping the domain name, only after jsmith cannot be found in corporation.com will Cisco Secure ACS use the Domain List and find the user in the engineering domain. The additional delay could be several seconds.
- **Enable PEAP machine authentication**—This check box controls whether Cisco Secure ACS performs machine authentication using machine name and password with PEAP(EAP-MSCHAPv2). For more information about machine authentication, see Machine Authentication, page 13-16.
- **Enable EAP-TLS machine authentication**—This check box controls whether Cisco Secure ACS performs machine authentication using machine name and password with EAP-TLS. For more information about machine authentication, see Machine Authentication, page 13-16.



Downloaded from www.Manualslib.com manuals search engine

- **EAP-TLS and PEAP machine authentication name prefix**—This box defines the string of characters that Cisco Secure ACS adds to the beginning of any machine name being authenticated. By default, the end-user client prefixes machine names with "host/". If any text is present in the PEAP machine authentication name prefix box, Cisco Secure ACS prefixes the machine name with this instead.

**Note** If you configure the EAP-TLS and PEAP machine authentication name prefix box with a string other than "host/", authentication may fail.

- **Enable machine access restrictions**—If you enable PEAP or EAP-TLS machine authentication, the "Enable machine access restrictions" check box controls whether Cisco Secure ACS restricts network access of users who access the network with computer that fail machine authentication. For more information about the MAR feature, see Machine Access Restrictions, page 13-19.

**Note** Be sure you have enabled the types of machine authentication that your Windows computers are configured to use—either PEAP machine authentication or EAP-TLS authentication, or both. If the MAR feature is enabled but Cisco Secure ACS does not perform machine authentication for a computer, EAP-TLS and Microsoft PEAP users accessing the network with that computer will be assigned to the group specified in the "Group map for successful user authentication without machine authentication" list.

**Tip** To enable machine access restrictions, you must specify a number greater than zero in the Aging time (hours) box.

- **Aging time (hours)**—This box specifies the number of hours that Cisco Secure ACS caches IETF RADIUS Calling-Station-Id attribute values from successful machine authentications, for use with the MAR feature. The default value is zero hours, which means that Cisco Secure ACS does not cache Calling-Station-Id values.



Downloaded from www.Manualslib.com manuals search engine

**Note** If you do not change the value of the Aging time (hours) box to something other than zero, all EAP-TLS and Microsoft PEAP users whose computers perform machine authentication are assigned to the group specified in the "Group map for successful user authentication without machine authentication" list.

**Tip** To clear the cache of Calling-Station-Id values, type **0** in the **Aging time (hours)** box and click **Submit**.

- **Group map for successful user authentication without machine authentication**—This list specifies the group profile that Cisco Secure ACS applies to a user accessing the network from a computer that has not passed machine authentication for longer than the number of hours specified in the Aging time (hours) box. To deny such users any access to the network, select <No Access> (which is the default setting).

  **Note** User profile settings always override group profile settings. If a user profile grants an authorization that is denied by the group specified in the "Group map for successful user authentication without machine authentication" list, Cisco Secure ACS grants the authorization.

# Configuring a Windows External User Database

For information about the options available on the Windows User Database Configuration page, see Windows User Database Configuration Options, page 13-26.

To configure Cisco Secure ACS to authenticate users against the Windows user database in the trusted domains of your network, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Configuration**.

Cisco Secure ACS displays a list of all possible external user database types.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** Click **Windows Database**.

If no Windows database configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

**Step 4** If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for Windows authentication in the box provided, or accept the default name in the box.

c. Click **Submit**.

Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

**Step 5** Click **Configure**.

The Windows User Database Configuration page appears.

**Step 6** As needed, configure the options in the following tables:

- Dialin Permission
- Domain List
- MS CHAP Settings
- EAP Settings

For information about the options on the Windows User Database Configuration page, see Windows User Database Configuration Options, page 13-26.

**Note** All the settings on the Windows User Database Configuration page are optional and need not be enabled unless you want to permit and configure the specific features they support.



Downloaded from www.Manualslib.com manuals search engine

**Step 7** Click **Submit**.

Cisco Secure ACS saves the Windows user database configuration you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 15-4. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "User Management".

# Generic LDAP

Cisco Secure ACS supports ASCII, PAP, EAP-TLS, PEAP(EAP-GTC), and EAP-FAST (phase two only) authentication via generic Lightweight Directory Access Protocol (LDAP) databases, such as Netscape Directory Services. Other authentication protocols are not supported with LDAP external user databases.

**Note** Authentication protocols not supported with LDAP databases may be supported by another type of external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-10.

Cisco Secure ACS supports group mapping for unknown users by requesting group membership information from LDAP user databases. For more information about group mapping for users authenticated with an LDAP user database, see Group Mapping by Group Set Membership, page 16-4.

Configuring Cisco Secure ACS to authenticate against an LDAP database has no effect on the configuration of the LDAP database. To manage your LDAP database, see your LDAP database documentation.

This section contains the following topics:

- Cisco Secure ACS Authentication Process with a Generic LDAP User Database, page 13-33
- Multiple LDAP Instances, page 13-33
- LDAP Organizational Units and Groups, page 13-34
- Domain Filtering, page 13-34



Downloaded from www.Manualslib.com manuals search engine

- LDAP Failover, page 13-36
- LDAP Configuration Options, page 13-37
- Configuring a Generic LDAP External User Database, page 13-43

# Cisco Secure ACS Authentication Process with a Generic LDAP User Database

Cisco Secure ACS forwards the username and password to an LDAP database using a TCP connection on a port that you specify. The LDAP database either passes or fails the authentication request from Cisco Secure ACS. Upon receiving the response from the LDAP database, Cisco Secure ACS instructs the requesting AAA client to grant or deny the user access, depending upon the response from the LDAP server.

Cisco Secure ACS grants authorization based on the Cisco Secure ACS group to which the user is assigned. While the group to which a user is assigned can be determined by information from the LDAP server, it is Cisco Secure ACS that grants authorization privileges.

# Multiple LDAP Instances

You can create more than one LDAP configuration in Cisco Secure ACS. By creating more than one LDAP configuration with different IP address or port settings, you can configure Cisco Secure ACS to authenticate using different LDAP servers or using different databases on the same LDAP server. Each primary server IP address and port configuration, along with the secondary server IP address and port configuration, forms an LDAP instance that corresponds to one Cisco Secure ACS LDAP configuration instance.

Cisco Secure ACS does not require that each LDAP instance corresponds to a unique LDAP database. You can have more than one LDAP configuration set to access the same database. This is useful when your LDAP database contains more than one subtree for users or groups. Because each LDAP configuration supports only one subtree directory for users and one subtree directory for groups, you must configure separate LDAP instances for each user directory subtree and group directory subtree combination for which Cisco Secure ACS should submit authentication requests.



Downloaded from www.Manualslib.com manuals search engine

For each LDAP instance, you can add or leave it out of the Unknown User Policy. For more information, see About Unknown User Authentication, page 15-4.

For each LDAP instance, you can establish unique group mapping. For more information, see Group Mapping by Group Set Membership, page 16-4.

Multiple LDAP instances is also important when you use domain filtering. For more information, see Domain Filtering, page 13-34.

# LDAP Organizational Units and Groups

LDAP groups do not need to have the same name as their corresponding Cisco Secure ACS groups. The LDAP group can be mapped to a Cisco Secure ACS group with any name you want to assign. For more information about how your LDAP database handles group membership, see your LDAP database documentation. For more information on LDAP group mappings and Cisco Secure ACS, see Chapter 16, "User Group Mapping and Specification".

# Domain Filtering

Using domain filtering, you can control which LDAP instance is used to authenticate a user based on domain-qualified usernames. Domain filtering is based on parsing the characters either at the beginning or end of a username submitted for authentication. Domain filtering provides you with greater control over the LDAP instance that Cisco Secure ACS submits any given user authentication request to. You also have control of whether usernames are submitted to an LDAP server with their domain qualifiers intact.

For example, when EAP-TLS authentication is initiated by a Windows XP client, Cisco Secure ACS receives the username in `username@domainname` format. When PEAP authentication is initiated by a Cisco Aironet end-user client, Cisco Secure ACS receives the username without a domain qualifier. If both clients are to be authenticated with an LDAP database that stores usernames without domain qualifiers, Cisco Secure ACS can strip the domain qualifier. If separate user accounts are maintained in the LDAP database—both domain-qualified and non-domain-qualified user accounts—Cisco Secure ACS can pass usernames to the LDAP database without domain filtering.



Downloaded from www.Manualslib.com manuals search engine

If you choose to make use of domain filtering, each LDAP configuration you create in Cisco Secure ACS can perform domain filtering in one of two ways:

- **Limiting users to one domain**—Per each LDAP configuration in Cisco Secure ACS, you can require that Cisco Secure ACS only attempts to authenticate usernames that are qualified with a specific domain name. This corresponds to the "Only process usernames that are domain qualified" option on the LDAP Configuration page. For more information about this option, see LDAP Configuration Options, page 13-37.

  With this option, each LDAP configuration is limited to one domain and to one type of domain qualification. You can specify whether Cisco Secure ACS strips the domain qualification before submitting the username to an LDAP server. If the LDAP server stores usernames in a domain-qualified format, you should not configure Cisco Secure ACS to strip domain qualifiers.

  Limiting users to one domain is useful when the LDAP server stores usernames differently per domain, either by user context or by how the username is stored in Cisco Secure ACS—domain qualified or non-domain qualified. The end-user client or AAA client must submit the username to Cisco Secure ACS in a domain-qualified format, otherwise Cisco Secure ACS cannot determine the user's domain and does not attempt to authenticate the user with the LDAP configuration that uses this form of domain filtering.

- **Allowing any domain but stripping domain qualifiers**—Per each LDAP configuration in Cisco Secure ACS, you can configure Cisco Secure ACS to attempt to strip domain qualifiers based on common domain-qualifier delimiting characters. This corresponds to the "Process all usernames after stripping domain name and delimiter" option on the LDAP Configuration page. For more information about this option, see LDAP Configuration Options, page 13-37.

  Cisco Secure ACS supports both prefixed and suffixed domain qualifiers. A single LDAP configuration can attempt to strip both prefixed and suffixed domain qualifiers; however, you can only specify one delimiting character each for prefixed and suffixed domain qualifiers. To support more than one type of domain-qualifier delimiting character, you can create more than one LDAP configuration in Cisco Secure ACS.

  Allowing usernames of any domain but stripping domain qualifiers is useful when the LDAP server stores usernames in a non-domain qualified format but the AAA client or end-user client submits the username to Cisco Secure ACS in a domain-qualified format.



Downloaded from www.Manualslib.com manuals search engine

**Note** With this option, Cisco Secure ACS submits usernames that are non-domain qualified, too. Usernames are not required to be domain qualified to be submitted to an LDAP server.

# LDAP Failover

Cisco Secure ACS supports failover between a primary LDAP server and secondary LDAP server. In the context of LDAP authentication with Cisco Secure ACS, failover applies when an authentication request fails because Cisco Secure ACS could not connect to an LDAP server, such as when the server is down or is otherwise unreachable by Cisco Secure ACS. To use this feature, you must define the primary and secondary LDAP servers on the LDAP Database Configuration page. Also, you must select the On Timeout Use Secondary check box. For more information about configuring an LDAP external user database, see Configuring a Generic LDAP External User Database, page 13-43.

If the On Timeout Use Secondary check box is selected, and if the first LDAP server that Cisco Secure ACS attempts to contact cannot be reached, Cisco Secure ACS always attempts to contact the other LDAP server. The first server Cisco Secure ACS attempts to contact may not always be the primary LDAP server. Instead, the first LDAP server that Cisco Secure ACS attempts to contact depends on the previous LDAP authentication attempt and on the value specified in the Failback Retry Delay box.

## Successful Previous Authentication with the Primary LDAP Server

If, on the previous LDAP authentication attempt, Cisco Secure ACS successfully connected to the primary LDAP server, Cisco Secure ACS attempts to connect to the primary LDAP server. If Cisco Secure ACS cannot connect to the primary LDAP server, Cisco Secure ACS attempts to connect to the secondary LDAP server.

If Cisco Secure ACS cannot connect with either LDAP server, Cisco Secure ACS stops attempting LDAP authentication for the user. If the user is an unknown user, Cisco Secure ACS tries the next external user database listed in the Unknown User Policy list. For more information about the Unknown User Policy list, see About Unknown User Authentication, page 15-4.



Downloaded from www.Manualslib.com manuals search engine

## Unsuccessful Previous Authentication with the Primary LDAP Server

If, on the previous LDAP authentication attempt, Cisco Secure ACS could not connect to the primary LDAP server, whether Cisco Secure ACS first attempts to connect to the primary server or secondary LDAP server for the current authentication attempt depends on the value in the Failback Retry Delay box. If the Failback Retry Delay box is set to 0 (zero), Cisco Secure ACS always attempts to connect to the primary LDAP server first. And if Cisco Secure ACS cannot connect to the primary LDAP server, Cisco Secure ACS then attempts to connect to the secondary LDAP server.

If the Failback Retry Delay box is set to a number other than zero, Cisco Secure ACS determines how many minutes have passed since the last authentication attempt using the primary LDAP server occurred. If more minutes have passed than the value specified in the Failback Retry Delay box, Cisco Secure ACS attempts to connect to the primary LDAP server first. And if Cisco Secure ACS cannot connect to the primary LDAP server, Cisco Secure ACS then attempts to connect to the secondary LDAP server.

If fewer minutes have passed than the value specified in the Failback Retry Delay box, Cisco Secure ACS attempts to connect to the secondary LDAP server first. And if Cisco Secure ACS cannot connect to the secondary LDAP server, Cisco Secure ACS then attempts to connect to the primary LDAP server.

If Cisco Secure ACS cannot connect to either LDAP server, Cisco Secure ACS stops attempting LDAP authentication for the user. If the user is an unknown user, Cisco Secure ACS tries the next external user database listed in the Unknown User Policy list. For more information about the Unknown User Policy list, see About Unknown User Authentication, page 15-4.

# LDAP Configuration Options

The LDAP Database Configuration page contains many options, presented in three tables:

- **Domain Filtering**—This table contains options for domain filtering. The settings in this table affect all LDAP authentication performed using this configuration, regardless of whether the authentication is handled by the primary or secondary LDAP server. For more information about domain filtering, see Domain Filtering, page 13-34



Downloaded from www.Manualslib.com manuals search engine

This table contains the following options:

- **Process all usernames**—When this option is selected, Cisco Secure ACS does not perform domain filtering on usernames before submitting them to the LDAP server for authentication.
- **Only process usernames that are domain qualified**—When this option is selected, Cisco Secure ACS only attempts authentication for usernames that are domain qualified for a single domain. You must specify the type of domain qualifier and the domain in the "Qualified by" and Domain options. Cisco Secure ACS only submits usernames that are qualified in the method specified in the "Qualified by" option and that are qualified with the username specified in the Domain Qualifier box. You can also specify whether Cisco Secure ACS removes the domain qualifier from usernames before submitting them to an LDAP server.
- **Qualified by**—When "Only process usernames that are domain qualified" is selected, this option specifies the type of domain qualification. If you select Prefix, Cisco Secure ACS only processes usernames that begin with the characters specified in the Domain Qualifier box. If you select Suffix, Cisco Secure ACS only processes usernames that end in the characters specified in the Domain Qualifier box.

**Note** Regardless of the domain qualifier type selected, the domain name must match the domain specified in the Domain Qualifier box.

- **Domain Qualifier**—When "Only process usernames that are domain qualified" is selected, this option specifies the domain name and delimiting character that must qualify usernames so Cisco Secure ACS can submit the username to an LDAP server. The Domain box accepts up to 512 characters; however, only one domain name and its delimiting character are permitted.

  For example, if the domain name is "mydomain", the delimiting character is "@", and Suffix is selected on the "Qualified by" list, the Domain box should contain "@mydomain". If the domain name is "yourdomain", the delimiting character is "\", and Prefix is selected on the "Qualified by" list, the Domain Qualifier box should contain "yourdomain\"



Downloaded from www.Manualslib.com manuals search engine

- **Strip domain before submitting username to LDAP server**—When "Only process usernames that are domain qualified" is selected, this option specifies whether Cisco Secure ACS removes the domain qualifier and its delimiting character before submitting a username to an LDAP server. For example, if the username is "jwiedman@domain.com", the stripped username is "jwiedman".
- **Process all usernames after stripping domain name and delimiter**—When this option is selected, Cisco Secure ACS submits all usernames to an LDAP server after attempting to strip domain names. Usernames that are not domain qualified are processed, too. Domain name stripping occurs as specified by the following two options.
- **Strip starting characters through the last *X* character**—When "Process all usernames after stripping domain name and delimiter" is selected, this option specifies that Cisco Secure ACS attempts to strip a prefixed domain qualifier. If, in the username, Cisco Secure ACS finds the delimiter character that is specified in the *X* box, it strips all characters from the beginning of the username through the delimiter character. If the username contains more than one of the characters specified in the *X* box, Cisco Secure ACS strips characters through the last occurrence of the delimiter character.

  For example, if the delimiter character is "\" and the username is "DOMAIN\echamberlain", Cisco Secure ACS submits "echamberlain" to an LDAP server.

**Note** The X box cannot contain the following special characters:
# ? " * > <
Cisco Secure ACS does not allow these characters in usernames; therefore, if any of these characters are in the X box, stripping fails.

- **Strip ending characters through the first *Y* character**—When "Process all usernames after stripping domain name and delimiter" is selected, this option specifies that Cisco Secure ACS attempts to strip a suffixed domain qualifier. If, in the username, Cisco Secure ACS finds the delimiter character that is specified in the *Y* box, it strips all characters from the delimiter character through the end of the username. If the username contains more than one of the character specified in the *Y* box, Cisco Secure ACS strips characters starting with the first occurrence of the delimiter character.



Downloaded from www.Manualslib.com manuals search engine

For example, if the delimiter character is "@" and the username is "jwiedman@domain", then Cisco Secure ACS submits "jwiedman" to an LDAP server.

**Note** The X box cannot contain the following special characters:
# ? " * > <
Cisco Secure ACS does not allow these characters in usernames; therefore, if any of these characters are in the X box, stripping fails.

- **Common LDAP Configuration**—This table contains options that apply to all LDAP authentication performed using this configuration. Cisco Secure ACS uses the settings in this section regardless of whether the authentication is handled by the primary or secondary LDAP server. This table contains the following options:
  - **User Directory Subtree**—The distinguished name (DN) for the subtree that contains all users. For example:

`ou=`*organizational unit*`[,ou=`*next organizational unit*`]o=corporation.com`

If the tree containing users is the base DN, type:

```
o=corporation.com
```

or

```
dc=corporation,dc=com
```

as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

  - **Group Directory Subtree**—The DN for the subtree that contains all groups. For example:

`ou=`*organizational unit*`[,ou=`*next organizational unit*`]o=corporation.com`

If the tree containing groups is the base DN, type:

```
o=corporation.com
```

or

```
dc=corporation,dc=com
```

as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.



Downloaded from www.Manualslib.com manuals search engine

- **UserObjectType**—The name of the attribute in the user record that contains the username. You can obtain this attribute name from your Directory Server. For more information, refer to your LDAP database documentation. Cisco Secure ACS provides default values that reflect the default configuration of a Netscape Directory Server. Confirm all values for these fields with your LDAP server configuration and documentation.
- **UserObjectClass**—The value of the LDAP "objectType" attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user, some of which are shared with other object types. This box should contain a value that is not shared.
- **GroupObjectType**—The name of the attribute in the group record that contains the group name.
- **GroupObjectClass**—A value of the LDAP "objectType" attribute in the group record that identifies the record as a group.
- **Group Attribute Name**—The name of the attribute of the group record that contains the list of user records that are a member of that group.
- **Server Timeout**—The number of seconds Cisco Secure ACS waits for a response from an LDAP server before determining that the connection with that server has failed.
- **On Timeout Use Secondary**—Whether Cisco Secure ACS performs failover of LDAP authentication attempts. For more information about the LDAP failover feature, see LDAP Failover, page 13-36.
- **Failback Retry Delay**—The number of minutes after the primary LDAP server fails to authenticate a user that Cisco Secure ACS resumes sending authentication requests to the primary LDAP server first. A value of 0 (zero) causes Cisco Secure ACS to always use the primary LDAP server first.

- **Primary and Secondary LDAP Servers**—The Primary LDAP Server table and the Secondary LDAP Server table enable you to identify the LDAP servers and make settings that are unique to each. The Secondary LDAP Server table does not need to be completed if you do not intend to use LDAP failover. These tables contain the following options:
  - **Hostname**—The name or IP address of the server that is running the LDAP software. If you are using DNS on your network, you can type the hostname instead of the IP address.



Downloaded from www.Manualslib.com manuals search engine

- **Port**—The TCP/IP port number on which the LDAP server is listening. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information by viewing those properties on the LDAP server. If you want to use secure authentication, port 636 is usually used.
- **LDAP Version**—Whether Cisco Secure ACS uses LDAP version 3 or version 2 to communicate with your LDAP database. If this check box is selected, Cisco Secure ACS uses LDAP version 3. If it is not selected, Cisco Secure ACS uses LDAP version 2.
- **Security**—Whether Cisco Secure ACS uses SSL to provide more secure communication with the LDAP server. If you do not enable SSL, user credentials are passed to the LDAP server in clear text.
- **Certificate Database Path**—The path to the `cert7.db` file. This file must contain the certificates for the server to be queried and the trusted CA. You can use a Netscape web browser to generate `cert7.db` files. For information about generating a `cert7.db` file, refer to Netscape documentation.

  To perform secure authentication using SSL, you must provide a `cert7.db` certificate database file. Cisco Secure ACS requires a certificate database so that it can establish the SSL connection. The certificate database must be local to the Cisco Secure ACS Windows server.

  Cisco Secure ACS requires a `cert7.db` certificate database file for each LDAP server you configure. For example, to support users distributed in multiple LDAP trees, you could configure two LDAP instances in Cisco Secure ACS that would communicate with the same LDAP servers. Each LDAP instance would have a primary and a secondary LDAP server. Even though the two LDAP configurations share the same primary server, each LDAP configuration requires that you download a certificate database file to Cisco Secure ACS.

**Note** The database must be a `cert7.db` certificate database file. No other filename is supported.



Downloaded from www.Manualslib.com manuals search engine

– **Admin DN**—The DN of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory Subtree. It must contain the following information about your LDAP server:

  **uid=***user id*,[ou=*organizational unit*,][ou=*next organizational unit*]o=*organization*

  where *user id* is the username, *organizational unit* is the last level of the tree, and *next organizational unit* is the next level up the tree.

  For example:

  ```
  uid=joesmith,ou=members,ou=administrators,o=cisco
  ```

  You can use anonymous credentials for the administrator username if the LDAP server is configured to make the group name attribute visible in searches by anonymous credentials. Otherwise, you must specify an administrator username that permits the group name attribute to be visible to searches.

**Note** If the administrator username specified does not have permission to see the group name attribute in searches, group mapping fails for users authenticated by LDAP.

– **Password**—The password for the administrator account specified in the Admin DN box. Password case sensitivity is determined by the LDAP server.

# Configuring a Generic LDAP External User Database

Creating a generic LDAP configuration provides Cisco Secure ACS information that enables it to pass authentication requests to an LDAP database. This information reflects the way you have implemented your LDAP database and does not dictate how your LDAP database is configured or functions. For information about your LDAP database, refer to your LDAP documentation.

### Before You Begin

For information about the options on the LDAP Database Configuration page, see LDAP Configuration Options, page 13-37.



Downloaded from www.Manualslib.com manuals search engine

To configure Cisco Secure ACS to use the LDAP User Database, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Configuration**.

Cisco Secure ACS displays a list of all possible external user database types.

**Step 3** Click **Generic LDAP**.

**Note** The user authenticates against only one LDAP database.

If no LDAP database configuration exists, only the Database Configuration Creation table appears. Otherwise, in addition to the Database Configuration Creation table, the External User Database Configuration table appears.

**Step 4** If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for generic LDAP in the box provided.

c. Click **Submit**.

Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

**Step 5** Under External User Database Configuration, select the name of the LDAP database you need to configure.

**Note** If only one LDAP configuration exists, the name of that configuration appears instead of the list. Proceed to Step 6.

**Step 6** Click **Configure**.

**Caution** If you click Delete, the configuration of the selected LDAP database is deleted.

**Step 7** If you do not want Cisco Secure ACS to filter LDAP authentication requests by username, under Domain Filtering, select **Process all usernames**.



Downloaded from www.Manualslib.com manuals search engine

**Step 8** If you want to limit authentications processed by this LDAP configuration to usernames with a specific domain qualification, follow these steps:

**Note** For information about domain filtering, see Domain Filtering, page 13-34.

a. Under Domain Filtering, select **Only process usernames that are domain qualified**.

b. From the "Qualified by" list, select the applicable type of domain qualification, either Suffix or Prefix. Only one type of domain qualification is supported per LDAP configuration.

   For example, if you want this LDAP configuration to authenticate usernames that begin with a specific domain name, select Prefix. If you want this LDAP configuration to authenticate usernames that end with a specific domain name, select Suffix.

c. In the Domain Qualifier box, type the name of the domain that you want this LDAP configuration to authenticate usernames for. Include the delimiting character that separates the user ID from the domain name. Be sure that the delimiting character appears in the applicable position: at the end of the domain name if Prefix is selected on the "Qualified by" list; at the beginning of the domain name if Suffix is selected on the "Qualified by" list.

   Only one domain name is supported per LDAP configuration. You can type up to 512 characters.

d. If you want Cisco Secure ACS to remove the domain qualifier before submitting it to the LDAP database, select the **Strip domain before submitting username to LDAP server** check box.

e. If you want Cisco Secure ACS to pass the username to the LDAP database *without* removing the domain qualifier, clear the **Strip domain before submitting username to LDAP server** check box.

**Step 9** If you want to enable Cisco Secure ACS to strip domain qualifiers from usernames before submitting them to an LDAP server, follow these steps:



Downloaded from www.Manualslib.com manuals search engine

**Note** For information about domain filtering, see Domain Filtering, page 13-34.

a. Under Domain Filtering, select **Process all usernames after stripping domain name and delimiter**.

b. If you want Cisco Secure ACS to strip prefixed domain qualifiers, select the **Strip starting characters through the last** *X* **character** check box, and then type the domain-qualifier delimiting character in the *X* box.

**Note** The X box cannot contain the following special characters:
# ? " * > <
If any of these characters are in the X box, stripping fails.

c. If you want Cisco Secure ACS to strip suffixed domain qualifiers, select the **Strip ending characters from the first** *X* **character** check box, and then type the domain-qualifier delimiting character in the *X* box.

**Note** The X box cannot contain the following special characters:
# ? " * > <
If any of these characters are in the X box, stripping fails.

**Step 10** Under Common LDAP Configuration, in the User Directory Subtree box, type the DN of the tree containing all your users.

**Step 11** In the Group Directory Subtree box, type the DN of the subtree containing all your groups.

**Step 12** In the User Object Type box, type the name of the attribute in the user record that contains the username. You can obtain this attribute name from your Directory Server. For more information, refer to your LDAP database documentation.

**Note** The default values in the UserObjectType and following fields reflect the default configuration of the Netscape Directory Server. Confirm all values for these fields with your LDAP server configuration and documentation.



Downloaded from www.Manualslib.com manuals search engine

**Step 13** In the User Object Class box, type the value of the LDAP "objectType" attribute that identifies the record as a user. Often, user records have several values for the objectType attribute, some of which are unique to the user, some of which are shared with other object types. Select a value that is not shared.

**Step 14** In the GroupObjectType box, type the name of the attribute in the group record that contains the group name.

**Step 15** In the GroupObjectClass box, type a value of the LDAP "objectType" attribute in the group record that identifies the record as a group.

**Step 16** In the GroupAttributeName box, type the name of the attribute of the group record that contains the list of user records who are a member of that group.

**Step 17** In the Server Timeout box, type the number of seconds Cisco Secure ACS waits for a response from an LDAP server before determining that the connection with that server has failed.

**Step 18** To enable failover of LDAP authentication attempts, select the **On Timeout Use Secondary** check box. For more information about the LDAP failover feature, see LDAP Failover, page 13-36.

**Step 19** In the Failback Retry Delay box, type the number of minutes after the primary LDAP server fails to authenticate a user that Cisco Secure ACS resumes sending authentication requests to the primary LDAP server first.

**Note** To specify that Cisco Secure ACS should always use the primary LDAP server first, type **0** (zero) in the Failback Retry Delay box.



Downloaded from www.Manualslib.com manuals search engine

**Step 20** For the Primary LDAP Server and Secondary LDAP Server tables, follow these steps:

**Note** If you did not select the On Timeout Use Secondary check box, you do not need to complete the options in the Secondary LDAP Server table.

a. In the Hostname box, type the name or IP address of the server that is running the LDAP software. If you are using DNS on your network, you can type the hostname instead of the IP address.

b. In the Port box, type the TCP/IP port number on which the LDAP server is listening. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information by viewing those properties on the LDAP server. If you want to use secure authentication, port 636 is usually used.

c. To specify that Cisco Secure ACS should use LDAP version 3 to communicate with your LDAP database, select the **LDAP Version** check box. If the LDAP Version check box is not selected, Cisco Secure ACS uses LDAP version 2.

d. The username and password credentials are normally passed over the network to the LDAP directory in clear text. To enhance security, select the **Use secure authentication** check box.

e. In the Certificate Database Path box, type the path to the `cert7.db` file, which contains the certificates for the server to be queried and the trusted CA.

f. The Admin DN box requires the fully qualified (DN) of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory Subtree.

In the Admin DN box, type the following information from your LDAP server:

**`uid=`***user id*`,[ou=`*organizational unit*`,]`
`[ou=`*next organizational unit*`]o=`*organization*

where *user id* is the username

*organizational unit* is the last level of the tree

*next organizational unit* is the next level up the tree.



Downloaded from www.Manualslib.com manuals search engine

For example:

```
uid=joesmith,ou=members,ou=administrators,o=cisco
```

**Tip** If you are using Netscape DS as your LDAP software, you can copy this information from the Netscape Console.

For more information, refer to your LDAP database documentation.

g. In the Password box, type the password for the administrator account specified in the Admin DN box. Password case sensitivity is determined by the server.

**Step 21** Click **Submit**.

Cisco Secure ACS saves the generic LDAP configuration you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 15-4. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "User Management".

# Novell NDS Database

Cisco Secure ACS supports user authentication with Novell NetWare Directory Services (NDS) servers.

This section contains the following topics:


- About Novell NDS User Databases, page 13-50
- User Contexts, page 13-51
- Novell NDS External User Database Options, page 13-52
- Configuring a Novell NDS External User Database, page 13-53




Downloaded from www.Manualslib.com manuals search engine

# About Novell NDS User Databases

Cisco Secure ACS supports ASCII, PAP, and PEAP(EAP-GTC) authentication with Novell NetWare Directory Services (NDS) servers. To use NDS authentication, you must have a Novell NDS database. Other authentication protocols are not supported with Novell NDS external user databases.

**Note** Authentication protocols not supported with Novell NDS external user databases may be supported by another type of external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-10.

Cisco Secure ACS supports group mapping for unknown users by requesting group membership information from Novell NDS user databases. For more information about group mapping for users authenticated with a Novell NDS user database, see Group Mapping by Group Set Membership, page 16-4.

**Note** Aside from user group membership information, Cisco Secure ACS retrieves no user settings from Novell NDS databases; however, Cisco Secure ACS enforces password restrictions, login restrictions, time restrictions, and account restrictions for each user. Cisco Secure ACS accomplishes this by interpreting authentication responses received from a Novell NDS database. Cisco Secure ACS does not enforce address restrictions.

Configuring Cisco Secure ACS to authenticate against an NDS database does not affect the configuration of the NDS database. To manage your NDS database, refer to your NDS database documentation.

Some versions of Novell NDS provide standard LDAP implementations. If your Novell NDS supports standard LDAP and you have implemented standard LDAP, you should configure a Cisco Secure ACS generic LDAP external user database to authenticate users defined in your Novell NDS. For more information about generic LDAP external user databases, see Generic LDAP, page 13-32.

To authenticate users with a Novell NDS database, Cisco Secure ACS depends upon Novell Requestor. Novell Requestor must be installed on the same Windows server as Cisco Secure ACS. You can download the Requestor software from the Novell website. For more information, refer to your Novell and Microsoft documentation.



Downloaded from www.Manualslib.com manuals search engine

For users to authenticate against a Novell NDS database, Cisco Secure ACS must be correctly configured to recognize the Novell NDS structure. Cisco Secure ACS supports up to twenty Novell NDS trees. Each Novell NDS tree configuration can support a list of user contexts. For a user to authenticate against a Novell NDS context, the applicable user object must exist in one of the contexts provided and the user password must be able to log the name into the tree.

# User Contexts

You must supply one or more contexts when you configure Cisco Secure ACS to authenticate with an NDS database; however, users can supply an additional portion of the full context that defines their fully qualified usernames. In other words, if none of the contexts in the list of contexts contains a username submitted for authentication, the username must specify exactly how they are subordinate to the contexts in the list of contexts. The user specifies the manner in which a username is subordinate to a context by providing the additional context information needed to uniquely identify the user in the NDS database.

Consider the following example tree:

```
[Root] whose treename=ABC
 OU=ABC-Company
  OU=sales
     CN=Agamemnon
  OU=marketing
    CN=Odysseus
    OU=marketing-research
       CN=Penelope
    OU=marketing-product
       CN=Telemachus
```

If the context list configured in Cisco Secure ACS were:

```
ABC-Company,sales.ABC-Company
```

Agamemnon would successfully authenticate if he submitted “Agamemnon.sales” as his username. If he submitted only “Agamemnon”, authentication would fail.

Table 13-1 lists the users given in the example tree and the username with context that would allow each user to authenticate successfully.



Downloaded from www.Manualslib.com manuals search engine

*Table 13-1 Example Usernames with Contexts*

| User | Valid Username With Context |
|---|---|
| Agamemnon | Agamemnon |
| Odysseus | Odysseus.marketing |
| Penelope | Penelope.marketing-research.marketing |
| Telemachus | Telemachus.marketing-product.marketing |

# Novell NDS External User Database Options

You create and maintain configurations for Novell NDS database authentication on the NDS Authentication Support page in Cisco Secure ACS. This page enables you to add a configuration for a Novell NDS tree, change existing tree configurations, and delete existing tree configurations in a single submission to the Cisco Secure ACS web server. Cisco Secure ACS displays information for each tree configured, plus a blank section for creating a tree. The configuration items presented for each tree are as follows:

- **Add New Tree**—Appears only on the blank form for new trees. Selecting this check box confirms that you want to add a new tree.
- **Delete Tree**—Appears only on existing tree configurations. Selecting this check box indicates that you want to delete the tree configuration when you click Submit.
- **Test Login**—Selecting this check box causes Cisco Secure ACS to test the administrative login of the tree to the Novell server when you click Submit.
- **Tree Name**—Appears only on the blank form for new trees. The name of the Novell NDS tree against which Cisco Secure ACS should authenticate users.
- **Administrator Username**—The fully qualified, typeless username for the administrator of the Novell server. For example:

  ```
  admin.Chicago.Corporation
  ```

  You can use anonymous credentials for the administrator username if the Novell NDS server is configured to make the group name attribute visible in searches by anonymous credentials. Otherwise, you must specify a administrator username that permits the group name attribute to be visible to searches.



Downloaded from www.Manualslib.com manuals search engine

**Note** If the administrator username specified does not have permission to see the group name attribute in searches, group mapping fails for users authenticated by Novell NDS.

- **Administrator Password**—The password for the administrator of the Novell server.
- **Context List**—The full context list with each context specified in canonical, typeless form; that is, remove the `o=` and `ou=` and separate each part of the context using a period (.). You can enter more than one context list. If you do, separate them with a comma. For example, if your Organization is Corporation, your Organization Name is Chicago, and you want to enter two Context names, Marketing and Engineering, you would type:

  ```
  Engineering.Chicago.Corporation,Marketing.Chicago.Corporation
  ```

  You do not need to add users in the Context List box.

  **Note** Users can provide a portion of their context when they login. For more information, see User Contexts, page 13-51.

- **Context Subtree**—Selecting this check box causes Cisco Secure ACS to search subtrees for users during authentication. The subtrees searched are those of the contexts specified in the Context List box.

# Configuring a Novell NDS External User Database

Creating an Novell NDS database configuration is a process that provides Cisco Secure ACS information that enables it to pass authentication requests to an NDS database. This information reflects the way you have implemented your NDS database and does not dictate how your NDS database is configured or functions. For information about your NDS database, refer to your Novell NDS documentation.

**Tip** You can allow users to enter their own context as part of the login process. For more information, see User Contexts, page 13-51.



Downloaded from www.Manualslib.com manuals search engine

### Before You Begin

The Novell Requestor Software for Novell NDS must be installed on the same computer as Cisco Secure ACS. If the Novell Requestor Software for Novell NDS is not on the same computer as Cisco Secure ACS, you cannot complete this procedure.

To configure Novell NDS authentication, follow these steps:

**Step 1** See your Novell NetWare administrator to get the names and other information on the Tree, Container, and Context.

**Step 2** In the navigation bar, click **External User Databases**.

**Step 3** Click **Database Configuration**.

Cisco Secure ACS lists all possible external user database types.

**Step 4** Click **Novell NDS**.

If no Novell NDS database has yet been configured, the Database Configuration Creation page appears. Otherwise, the External User Database Configuration page appears.

**Step 5** If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for Novell NDS Authentication in the box provided.

c. Click **Submit**.

Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

**Step 6** Click **Configure**.

**Caution** If you click Delete, the Cisco Secure ACS configuration for your Novell NDS database is deleted.

The NDS Authentication Support page appears. The NDS Authentication Support page enables you to add a configuration for a Novell NDS server, change existing Novell NDS server configurations, and delete existing Novell NDS server configurations.



Downloaded from www.Manualslib.com manuals search engine

For more information about the content of the NDS Authentication Support page, see Novell NDS External User Database Options, page 13-52.

**Step 7** If you want to add a new Novell NDS server configuration, complete the fields in the blank form at the bottom of the NDS Authentication Support page.

**Note** You must select the Add New NDS Host check box to confirm that you want to create a Novell NDS server configuration.

**Step 8** If you want to change an existing tree configuration, edit the values you need to change.

**Note** The name of a tree is not changeable. If you need to change a tree name, click **Delete Tree?** on the misnamed tree section and click **Submit**. Then, add a new tree with the same configuration data as the deleted, misnamed tree, making sure the tree name is correct before clicking Submit.

**Step 9** If you want to delete an existing tree configuration, select the **Delete Tree** check box.

**Step 10** Click **Submit**.

Cisco Secure ACS saves the NDS configuration you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 15-4. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "User Management".

# ODBC Database

As with Windows user database support, Cisco Secure ACS ODBC-compliant relational database support enables you to make use of existing user records held in an external ODBC-compliant relational database. Configuring Cisco Secure



Downloaded from www.Manualslib.com manuals search engine

ACS to authenticate against an ODBC-compliant relational database does not affect the configuration of the relational database. To manage your relational database, refer to your relational database documentation.

**Note** As with all other external databases supported by Cisco Secure ACS, the ODBC-compliant relational database is not supplied as part of Cisco Secure ACS. For general guidance with setting up your ODBC external user database, see Preparing to Authenticate Users with an ODBC-Compliant Relational Database, page 13-59.

The Windows ODBC feature enables you to create a data source name (DSN), which specifies the database and other important parameters necessary for communicating with the database. Among the parameters you provide are the username and password required for the ODBC driver to gain access to your ODBC-compliant relational database.

This section contains the following topics:


- What is Supported with ODBC User Databases, page 13-57
- Cisco Secure ACS Authentication Process with an ODBC External User Database, page 13-58
- Preparing to Authenticate Users with an ODBC-Compliant Relational Database, page 13-59
- Implementation of Stored Procedures for ODBC Authentication, page 13-60
- Microsoft SQL Server and Case-Sensitive Passwords, page 13-61
- Sample Routine for Generating a PAP Authentication SQL Procedure, page 13-62
- Sample Routine for Generating an SQL CHAP Authentication Procedure, page 13-63
- Sample Routine for Generating an EAP-TLS Authentication Procedure, page 13-64
- PAP Authentication Procedure Input, page 13-64
- PAP Procedure Output, page 13-65
- CHAP/MS-CHAP/ARAP Authentication Procedure Input, page 13-66
- CHAP/MS-CHAP/ARAP Procedure Output, page 13-66




Downloaded from www.Manualslib.com manuals search engine

- EAP-TLS Authentication Procedure Input, page 13-67
- EAP-TLS Procedure Output, page 13-68
- Result Codes, page 13-69
- Configuring a System Data Source Name for an ODBC External User Database, page 13-70
- Configuring an ODBC External User Database, page 13-71


# What is Supported with ODBC User Databases

Cisco Secure ACS supports the use of ODBC external user databases for the following features:

- **Authentication**—Cisco Secure ACS supports ASCII, PAP, ARAP, CHAP, MS-CHAP (versions 1 and 2), LEAP, EAP-TLS, EAP-MD5, PEAP(EAP-GTC), and EAP-FAST (phase zero and phase two) authentication using a relational database via the ODBC authenticator feature. Other authentication protocols are not supported with ODBC external user databases.

  **Note** Authentication protocols not supported with ODBC external user databases may be supported by another type of external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-10.

- **Group Specification**—Cisco Secure ACS supports group assignment for users authenticated by an ODBC user database. Authentication queries to the ODBC database must contain the group number you want to assign a user to. For unknown users authenticated by an ODBC user database, group specification overrides group mapping.

  For more information about expected query output, see PAP Procedure Output, page 13-65, CHAP/MS-CHAP/ARAP Procedure Output, page 13-66, and EAP-TLS Procedure Output, page 13-68.



Downloaded from www.Manualslib.com manuals search engine

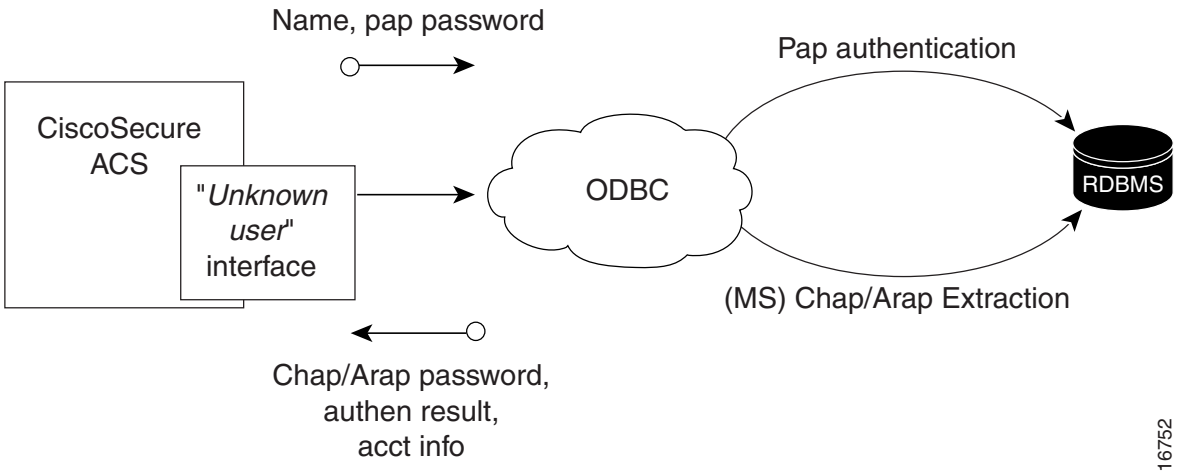
- **Group Mapping for Unknown Users**—Cisco Secure ACS supports group mapping for unknown users by requesting group membership information from Windows user databases. For more information about group mapping for users authenticated with a Windows user database, see Group Mapping by Group Set Membership, page 16-4.

# Cisco Secure ACS Authentication Process with an ODBC External User Database

Cisco Secure ACS forwards user authentication requests to an ODBC database in either of the two following scenarios. The first scenario is when the user account in the CiscoSecure user database lists an ODBC database configuration as the authentication method. The second is when the user is unknown to the CiscoSecure user database and the Unknown User Policy dictates that an ODBC database is the next external user database to try.

In either case, Cisco Secure ACS forwards user credentials to the ODBC database via an ODBC connection. The relational database must have a stored procedure that queries the appropriate tables and returns values to Cisco Secure ACS. If the returned values indicate that the user credentials provided are valid, Cisco Secure ACS instructs the requesting AAA client to grant the user access; otherwise, Cisco Secure ACS denies the user access (Figure 13-2).

***Figure 13-2 Using the ODBC Database for Authentication***






Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS grants authorization based on the Cisco Secure ACS group to which the user is assigned. While the group to which a user is assigned can be determined by information from the ODBC database using a process known as "group specification", it is Cisco Secure ACS that grants authorization privileges.

# Preparing to Authenticate Users with an ODBC-Compliant Relational Database

Authenticating users with an ODBC-compliant relational database requires that you complete several significant steps external to Cisco Secure ACS before configuring Cisco Secure ACS with an ODBC external user database.

To prepare for authenticating with an ODBC-compliant relational database, follow these steps:

**Step 1** Install your ODBC-compliant relational database on its server. For more information, refer to the relational database documentation.

**Note** The relational database you use is not supplied with Cisco Secure ACS.

**Step 2** Create the database to hold the usernames and passwords. The database name is irrelevant to Cisco Secure ACS, so you can name the database however you like.

**Step 3** Create the table or tables that will hold the usernames and passwords for your users. The table names are irrelevant to Cisco Secure ACS, so you can name the tables and columns however you like.

**Note** For SQL database columns that hold user passwords, we recommend using varchar format. If you define password columns as char, password comparison may fail if the password does not use the full length of the field. For example, if a password column is 16 characters wide but the password is only ten characters long, the database may append six spaces make the value used for password comparison 16 characters long, causing comparison to the actual password submitted by the user to fail.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** Write the stored procedures intended to return the required authentication information to Cisco Secure ACS. For more information about these stored procedures, see Implementation of Stored Procedures for ODBC Authentication, page 13-60.

**Step 5** Set up a system DSN on the computer running Cisco Secure ACS. For steps, see Configuring a System Data Source Name for an ODBC External User Database, page 13-70.

**Step 6** Configure Cisco Secure ACS to authenticate users with an ODBC database. For steps, see Configuring an ODBC External User Database, page 13-71.

# Implementation of Stored Procedures for ODBC Authentication

When you configure Cisco Secure ACS to authenticate users against an ODBC-compliant relational database, you must create a stored procedure to perform the necessary query and return the values that Cisco Secure ACS expects. The values returned and the tasks required of the stored procedure varies depending upon the authentication protocol used.

Authentication for ASCII, PAP, or PEAP (EAP-GTC) occurs within the relational database; that is, if the stored procedure finds a record with both the username and the password matching the input, the user is considered authenticated.

Authentication for CHAP, MS-CHAP, ARAP, LEAP, or EAP-MD5 occurs within Cisco Secure ACS. The stored procedure returns the fields for the record with a matching username, including the password. Cisco Secure ACS confirms or denies authentication based on the values returned from the procedure.

Authentication for EAP-TLS occurs within Cisco Secure ACS. The stored procedure returns the field for the record, indicating whether it found the username in the ODBC database. Cisco Secure ACS confirms or denies authentication based on the values returned from the procedure and upon the validity of the user certificate. For more information about Cisco Secure ACS support for the EAP-TLS protocol, see EAP-TLS Authentication, page 10-2.

To support the three sets of protocols, Cisco Secure ACS provides different input to, and expects different output from, the ODBC authentication request. This requires a separate stored procedure in the relational database to support each of the three sets of protocols.



Downloaded from www.Manualslib.com manuals search engine

The Cisco Secure ACS product CD provides "stub" routines for creating a procedure in either Microsoft SQL Server or an Oracle database. You can either modify a copy of these routines to create your stored procedure or write your own. Example routines for creating PAP and CHAP/MS-CHAP/ARAP authentication stored procedures in SQL Server are given in Sample Routine for Generating a PAP Authentication SQL Procedure, page 13-62, and Sample Routine for Generating an SQL CHAP Authentication Procedure, page 13-63.

The following sections provide reference information about Cisco Secure ACS data types versus SQL data types, ASCII/PAP/PEAP(EAP-GTC) authentication procedure input and output, CHAP/MS-CHAP/ARAP authentication procedure input and output, EAP-TLS authentication procedure input and output, and expected result codes. You can use this information while writing your authentication stored procedures in your relational database.

## Type Definitions

The Cisco Secure ACS types and their matching SQL types are as follows:

- **Integer**—SQL_INTEGER
- **String**—SQL_CHAR or SQL_VARCHAR

**Note** For SQL database columns that hold user passwords, we recommend using varchar format. If you define password columns as char, password comparison may fail if the password does not use the full length of the field. For example, if a password column is 16 characters wide but the password is only ten characters long, the database may append six spaces make the value used for password comparison 16 characters long, causing comparison to the actual password submitted by the user to fail.

# Microsoft SQL Server and Case-Sensitive Passwords

If you want your passwords to be case sensitive and are using Microsoft SQL Server as your ODBC-compliant relational database, configure your SQL Server to accommodate this feature. If your users are authenticating using PPP via PAP or Telnet login, the password might not be case sensitive, depending on how the case-sensitivity option is set on the SQL Server. For example, an Oracle database



Downloaded from www.Manualslib.com manuals search engine

will default to case sensitive, whereas Microsoft SQL Server defaults to case insensitive. However, in the case of CHAP/ARAP, the password is case sensitive if the CHAP stored procedure is configured.

For example, with Telnet or PAP authentication, the passwords **cisco** or **CISCO** or **CiScO** will all work if the SQL Server is configured to be case insensitive.

For CHAP/ARAP, the passwords **cisco** or **CISCO** or **CiScO** are not the same, regardless of whether or not the SQL Server is configured for case-sensitive passwords.

# Sample Routine for Generating a PAP Authentication SQL Procedure

The following example routine creates a procedure named CSNTAuthUserPap in Microsoft SQL Server, the default procedure used by Cisco Secure ACS for PAP authentication. Table and column names that could vary for your database schema are presented in variable text. For your convenience, the Cisco Secure ACS product CD includes a stub routine for creating a procedure in either SQL Server or Oracle. For more information about data type definitions, procedure parameters, and procedure results, see ODBC Database, page 13-55.

```
if exists (select * from sysobjects where id = object_id (`dbo.CSNTAuthUserPap') and
sysstat & 0xf = 4)
drop procedure dbo.CSNTAuthUserPap
GO

CREATE PROCEDURE CSNTAuthUserPap
@username varchar(64), @pass varchar(255)
AS
SET NOCOUNT ON
IF EXISTS( SELECT  username
FROM  users
WHERE  username  = @username
AND  csntpassword  = @pass )
SELECT 0,csntgroup,csntacctinfo,"No Error"
FROM  users
WHERE  username  = @username
ELSE
SELECT 3,0,"odbc","ODBC Authen Error"
GO
```



Downloaded from www.Manualslib.com manuals search engine

```
GRANT EXECUTE ON dbo.CSNTAuthUserPap TO ciscosecure
GO
```

# Sample Routine for Generating an SQL CHAP Authentication Procedure

The following example routine creates in Microsoft SQL Server a procedure named CSNTExtractUserClearTextPw, the default procedure used by Cisco Secure ACS for CHAP/MS-CHAP/ARAP authentication. Table and column names that could vary for your database schema are presented in variable text. For more information about data type definitions, procedure parameters, and procedure results, see ODBC Database, page 13-55.

```
 if exists (select * from sysobjects where id =
object_id(`dbo.CSNTExtractUserClearTextPw') and sysstat & 0xf = 4)
drop procedure dbo.CSNTExtractUserClearTextPw
GO

CREATE PROCEDURE CSNTExtractUserClearTextPw
@username varchar(64)
AS
SET NOCOUNT ON
IF EXISTS( SELECT  username
FROM  users
WHERE  username  = @username )
SELECT 0,csntgroup,csntacctinfo,"No Error",csntpassword
FROM  users
WHERE  username  = @username
ELSE
SELECT 3,0,"odbc","ODBC Authen Error"
GO

GRANT EXECUTE ON dbo.CSNTExtractUserClearTextPw TO ciscosecure
GO
```



Downloaded from www.Manualslib.com manuals search engine

# Sample Routine for Generating an EAP-TLS Authentication Procedure

The following example routine creates in Microsoft SQL Server a procedure named CSNTFindUser, the default procedure used by Cisco Secure ACS for EAP-TLS authentication. Table and column names that could vary for your database schema are presented in variable text. For more information about data type definitions, procedure parameters, and procedure results, see ODBC Database, page 13-55.

```
if exists (select * from sysobjects where id = object_id(`dbo.CSNTFindUser') and sysstat &
0xf = 4)
drop procedure dbo.CSNTFindUser
GO

CREATE PROCEDURE CSNTFindUser
@username varchar(64)
AS
SET NOCOUNT ON
IF EXISTS( SELECT  username
FROM  users
WHERE  username  = @username )
SELECT 0,csntgroup,csntacctinfo,"No Error"
FROM  users
WHERE  username  = @username
ELSE
SELECT 3,0,"odbc","ODBC Authen Error"
GO

GRANT EXECUTE ON dbo.CSNTFindUser TO ciscosecure
GO
```

# PAP Authentication Procedure Input

Table 13-2 details the input provided by Cisco Secure ACS to the stored procedure supporting PAP authentication. The stored procedure should accept the named input values as variables.



Downloaded from www.Manualslib.com manuals search engine

*Table 13-2 PAP Stored Procedure Input*

| Field | Type | Explanation |
|---|---|---|
| CSNTusername | String | 0-64 characters |
| CSNTpassword | String | 0-255 characters |

The input names are for guidance only. Procedure variables created from them can have different names; however, they must be defined in the procedure in the order shown—the username must precede the password variable.

# PAP Procedure Output

The stored procedure must return a single row containing the non-null fields. Table 13-3 lists the procedure results Cisco Secure ACS expects as output from stored procedure.

*Table 13-3 PAP Stored Procedure Results*

| Field | Type | Explanation |
|---|---|---|
| CSNTresult | Integer | See Table 13-8. |
| CSNTgroup | Integer | The Cisco Secure ACS group number for authorization. 0xFFFFFFFF is used to assign the default value. Values other than 0-499 are converted to the default.<br>**Note** The group specified in the CSNTgroup field overrides group mapping configured for the ODBC external user database. |
| CSNTacctInfo | String | 0-16 characters. A customer-defined string that Cisco Secure ACS adds to subsequent account log file entries. |
| CSNTerrorString | String | 0-255 characters. A customer-defined string that Cisco Secure ACS writes to the CSAuth service log file if an error occurs. |

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The CSNTerrorString file is logged only after a failure (if the result is greater than or equal to 4).



Downloaded from www.Manualslib.com manuals search engine

**Note** If the ODBC database returns data in recordset format rather than in parameters, the procedure must return the result fields in the order listed above.

# CHAP/MS-CHAP/ARAP Authentication Procedure Input

Cisco Secure ACS provides a single value for input to the stored procedure supporting CHAP/MS-CHAP/ARAP authentication. The stored procedure should accept the named input value as a variable.

**Note** Because Cisco Secure ACS performs authentication for CHAP/MS-CHAP/ARAP, the user password is not an input (Table 13-4).

*Table 13-4 CHAP Stored Procedure Input*

| Field | Type | Explanation |
|---|---|---|
| CSNTusername | String | 0-64 characters |

The input name is for guidance only. A procedure variable created from it can have a different name.

# CHAP/MS-CHAP/ARAP Procedure Output

The stored procedure must return a single row containing the non-null fields. Table 13-5 lists the procedure results Cisco Secure ACS expects as output from stored procedure.



Downloaded from www.Manualslib.com manuals search engine

*Table 13-5 CHAP/MS-CHAP/ARAP Stored Procedure Results*

| Field | Type | Explanation |
|---|---|---|
| CSNTresult | Integer | See Table 13-8 Result Codes. |
| CSNTgroup | Integer | The Cisco Secure ACS group number for authorization. 0xFFFFFFFF is used to assign the default value. Values other than 0-499 are converted to the default.<br>**Note** The group specified in the CSNTgroup field overrides group mapping configured for the ODBC external user database. |
| CSNTacctInfo | String | 0-15 characters. A customer-defined string that Cisco Secure ACS adds to subsequent account log file entries. |
| CSNTerrorString | String | 0-255 characters. A customer-defined string that Cisco Secure ACS writes to the CSAuth service log file if an error occurs. |
| CSNTpassword | String | 0-255 characters. The password is authenticated by Cisco Secure ACS.<br>**Note** If the password field in the database is defined using a CHAR datatype rather than VARCHAR, the database may return a string 255 characters long, regardless of actual password length. We recommend using the VARCHAR datatype for the CHAP password field in your ODBC database. |

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The CSNTerrorString file is logged only after a failure (if the result is greater than or equal to 4).

**Note** If the ODBC database returns data in recordset format rather than in parameters, the procedure must return the result fields in the order listed above.

# EAP-TLS Authentication Procedure Input

Cisco Secure ACS provides a single value for input to the stored procedure supporting EAP-TLS authentication. The stored procedure should accept the named input value as a variable.



Downloaded from www.Manualslib.com manuals search engine

**Note** Because Cisco Secure ACS performs authentication for EAP-TLS, the user password is not an input (Table 13-4).

*Table 13-6 EAP-TLS Stored Procedure Input*

| Field | Type | Explanation |
|---|---|---|
| CSNTusername | String | 0-64 characters |

The input name is for guidance only. A procedure variable created from it can have a different name.

# EAP-TLS Procedure Output

The stored procedure must return a single row containing the non-null fields. Table 13-5 lists the procedure results Cisco Secure ACS expects as output from stored procedure.

*Table 13-7 EAP-TLS Stored Procedure Results*

| Field | Type | Explanation |
|---|---|---|
| CSNTresult | Integer | See Table 13-8 Result Codes. |
| CSNTgroup | Integer | The Cisco Secure ACS group number for authorization. 0xFFFFFFFF is used to assign the default value. Values other than 0-499 are converted to the default.<br>**Note** The group specified in the CSNTgroup field overrides group mapping configured for the ODBC external user database. |
| CSNTacctInfo | String | 0-15 characters. A customer-defined string that Cisco Secure ACS adds to subsequent account log file entries. |
| CSNTerrorString | String | 0-255 characters. A customer-defined string that Cisco Secure ACS writes to the CSAuth service log file if an error occurs. |



Downloaded from www.Manualslib.com manuals search engine

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The CSNTerrorString file is logged only after a failure (if the result is greater than or equal to 4).

**Note** If the ODBC database returns data in recordset format rather than in parameters, the procedure must return the result fields in the order listed above.

# Result Codes

You can set the result codes listed in Table 13-8.

***Table 13-8 Result Codes***

| Result Code | Meaning |
|---|---|
| 0 (zero) | Authentication successful |
| 1 | Unknown username |
| 2 | Invalid password |
| 3 | Unknown username or invalid password |
| 4+ | Internal error—authentication not processed |

The SQL procedure can decide among 1, 2, or 3 to indicate a failure, depending on how much information you want the failed authentication log files to include.

A return code of 4 or higher results in an authentication error event. These errors do not increment per-user failed attempt counters. Additionally, error codes are returned to the AAA client so it can distinguish between errors and failures and, if configured to do so, fall back to a backup AAA server.

Successful or failed authentications are not logged; general Cisco Secure ACS logging mechanisms apply. In the event of an error (CSNTresult equal to or less than 4), the contents of the CSNTerrorString are written to the Windows Event Log under the Application Log.



Downloaded from www.Manualslib.com manuals search engine

# Configuring a System Data Source Name for an ODBC External User Database

On the computer running Cisco Secure ACS, you must create a system DSN for Cisco Secure ACS to communicate with the relational database.

To create a system DSN for use with an ODBC external user database, follow these steps:

**Step 1** Using the local administrator account, log in to the computer running Cisco Secure ACS.

**Step 2** In Windows Control Panel, double-click the **ODBC Data Sources** icon.

**Step 3** Choose **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**

**Tip** If Control Panel is not expanded on the Start menu, choose **Start > Settings > Control Panel**, double-click **Administrative Tools**, and then double-click **Data Sources (ODBC)**.

The ODBC Data Source Administrator window appears.

**Step 4** Click the **System DSN** tab.

**Step 5** Click **Add**.

**Step 6** Select the driver you need to use with your new DSN, and then click **Finish**.

A dialog box displays fields requiring information specific to the ODBC driver you selected.

**Step 7** Type a descriptive name for the DSN in the Data Source Name box.

**Step 8** Complete the other fields required by the ODBC driver you selected. These fields may include information such as the IP address of the server on which the ODBC-compliant database runs.

**Step 9** Click **OK**.

The name you assigned to the DSN appears in the System Data Sources list.



Downloaded from www.Manualslib.com manuals search engine

**Step 10** Close the ODBC Data Source Administrator window and Windows Control Panel.

The system DSN to be used by Cisco Secure ACS for communication with the relational database is created on the computer running Cisco Secure ACS.

# Configuring an ODBC External User Database

Creating an ODBC database configuration provides Cisco Secure ACS information that enables it to pass authentication requests to an ODBC-compliant relational database. This information reflects the way you have implemented your relational database and does not dictate how your relational database is configured or functions. For information about your relational database, refer to your relational documentation.

**Note** Before performing this procedure, you should have completed the steps in Preparing to Authenticate Users with an ODBC-Compliant Relational Database, page 13-59.

To configure Cisco Secure ACS for ODBC authentication, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Configuration**.

Cisco Secure ACS lists all possible external user database types.

**Step 3** Click **External ODBC Database**.

**Step 4** If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for ODBC authentication in the box provided, or accept the default name in the box.

c. Click **Submit**.

Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

**Step 5** Click **Configure**.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** From the System DSN list, select the DSN that is configured to communicate with the ODBC-compliant relational database you want to use.

**Note** If you have not configured on the computer running Cisco Secure ACS a DSN for the relational database, do so before completing these steps. For more information about creating a DSN for Cisco Secure ACS ODBC authentication, see Configuring a System Data Source Name for an ODBC External User Database, page 13-70.

**Step 7** In the DSN Username box, type the username required to perform transactions with your ODBC database.

**Step 8** In the DSN Password box, type the password required to perform transactions with your ODBC database.

**Step 9** In the DSN Connection Retries box, type the number of times Cisco Secure ACS should try to connect to the ODBC database before timing out. The default is 3.

**Note** If you have connection problems when Windows starts, increase this value.

**Step 10** To change the ODBC worker thread count, in the ODBC Worker Threads box, type the number of ODBC worker threads. The maximum thread count is 10. The default is 1.

**Note** Increase the ODBC worker thread count only if the ODBC driver you are using is certified thread safe. For example, the Microsoft Access ODBC driver is not thread safe and can cause Cisco Secure ACS to become unstable if multiple threads are used. Where possible, Cisco Secure ACS queries the driver to find out if it is thread safe. The thread count to use is a factor of how long the DSN takes to execute the procedure and the rate at which authentications are required.



Downloaded from www.Manualslib.com manuals search engine

**Step 11** From the DSN Procedure Type list, select the type of output your relational database provides. Different databases return different output:

- **Returns Recordset**—The database returns a raw record set in response to an ODBC query. Microsoft SQL Server responds in this manner.
- **Returns Parameters**—The database returns a set of named parameters in response to an ODBC query. Oracle databases respond in this manner.

**Step 12** To support ASCII, PAP, or PEAP(EAP-GTC) authentication with the ODBC database, follow these steps:

a. Select the **Support PAP authentication** check box.

b. In the PAP SQL Procedure box, type the name of the PAP SQL procedure routine that runs on the ODBC server. The default value in this box is CSNTAuthUserPap. If you named the PAP SQL procedure something else, change this entry to match the name given to the PAP SQL procedure. For more information and an example routine, see Sample Routine for Generating a PAP Authentication SQL Procedure, page 13-62.

**Note** If you enabled PAP authentication, the PAP authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the PAP SQL Procedure box. If it does not, be sure to create it in the ODBC database before attempting to authenticate users against the ODBC database.

**Step 13** To support CHAP, MS-CHAP, ARAP, EAP-MD5, or LEAP authentication with the ODBC database, follow these steps:

a. Select the **Support CHAP/MS-CHAP/ARAP Authentication** check box.

b. In the CHAP SQL Procedure box, type the name of the CHAP SQL procedure routine on the ODBC server. The default value in this box is CSNTExtractUserClearTextPw. If you named the CHAP SQL procedure something else, change this entry to match the name given to the CHAP SQL procedure. For more information and an example routine, see Sample Routine for Generating an SQL CHAP Authentication Procedure, page 13-63.



Downloaded from www.Manualslib.com manuals search engine

**Note** If you enabled CHAP/MS-CHAP/ARAP authentication, the CHAP authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the PAP SQL Procedure box. If it does not, be sure to create it in the ODBC database before attempting to authenticate users against the ODBC database.

**Step 14** To support EAP-TLS authentication with the ODBC database, follow these steps:

a. Select the **Support EAP-TLS Authentication** check box.

b. In the EAP-TLS SQL Procedure box, type the name of the EAP-TLS SQL procedure routine on the ODBC server. The default value in this box is CSNTFindUser. If you named the EAP-TLS SQL procedure something else, change this entry to match the name given to the EAP-TLS SQL procedure. For more information and an example routine, see Sample Routine for Generating an EAP-TLS Authentication Procedure, page 13-64.

**Note** If you enabled EAP-TLS authentication, the EAP-TLS authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the EAP-TLS SQL Procedure box. If it does not, be sure to create it in the ODBC database before attempting to authenticate users against the ODBC database.

**Step 15** Click **Submit**.

Cisco Secure ACS saves the ODBC configuration you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 15-4. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "User Management".



Downloaded from www.Manualslib.com manuals search engine

# LEAP Proxy RADIUS Server Database

For Cisco Secure ACS-authenticated users accessing your network via Cisco Aironet devices, Cisco Secure ACS supports ASCII, PAP, MS-CHAP (versions 1 and 2), LEAP, and EAP-FAST (phase zero and phase two) authentication with a proxy RADIUS server. Other authentication protocols are not supported with LEAP Proxy RADIUS Server databases.

**Note** Authentication protocols not supported with LEAP Proxy RADIUS Server databases may be supported by another type of external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-10.

Cisco Secure ACS uses MS-CHAP version 1 for LEAP Proxy RADIUS Server authentication. To manage your proxy RADIUS database, refer to your RADIUS database documentation.

Lightweight extensible authentication protocol (LEAP) proxy RADIUS server authentication allows you to authenticate users against existing Kerberos databases that support MS-CHAP authentication. You can use the LEAP Proxy RADIUS Server database to authenticate users with any third-party RADIUS server that supports MS-CHAP authentication.

**Note** The third-party RADIUS server must return Microsoft Point-to-Point Encryption (MPPE) keys in the Microsoft RADIUS vendor-specific attribute (VSA) MSCHAP-MPPE-Keys (VSA 12). If the third-party RADIUS server does not return the MPPE keys, the authentication fails and is logged in the Failed Attempts log.

Cisco Secure ACS supports RADIUS-based group specification for users authenticated by LEAP Proxy RADIUS Server databases. RADIUS-based group specification overrides group mapping. For more information, see RADIUS-Based Group Specification, page 16-14.

Cisco Secure ACS supports group mapping for unknown users authenticated by LEAP Proxy RADIUS Server databases. Group mapping is only applied to an unknown user if RADIUS-based group specification did not occur. For more information about group mapping users authenticated by a LEAP Proxy RADIUS Server database, see Group Mapping by External User Database, page 16-2.



Downloaded from www.Manualslib.com manuals search engine

# Configuring a LEAP Proxy RADIUS Server External User Database

You should install and configure your proxy RADIUS server before configuring Cisco Secure ACS to authenticate users with it. For information about installing the proxy RADIUS server, refer to the documentation included with your RADIUS server.

To configure LEAP proxy RADIUS authentication, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Configuration**.

Cisco Secure ACS lists all possible external user database types.

**Step 3** Click **LEAP Proxy RADIUS Server**.

If no LEAP Proxy RADIUS Server configuration exists, only the Database Configuration Creation table appears. Otherwise, in addition to the Database Configuration Creation table, the External User Database Configuration table appears.

**Step 4** If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for the LEAP Proxy RADIUS Server in the box provided, or accept the default name in the box.

c. Click **Submit**.

Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

**Step 5** Under External User Database Configuration, select the name of the LEAP Proxy RADIUS Server database you need to configure.

**Note** If only one LEAP Proxy RADIUS Server configuration exists, the name of that configuration appears instead of the list. Proceed to Step 6.

**Step 6** Click **Configure**.



Downloaded from www.Manualslib.com manuals search engine

**Step 7** In the following boxes, type the required information:

- **Primary Server Name/IP**—IP address of the primary proxy RADIUS server.
- **Secondary Server Name/IP**—IP address of the secondary proxy RADIUS server.
- **Shared Secret**—The shared secret of the proxy RADIUS server. This must be identical to the shared secret with which the proxy RADIUS server is configured.
- **Authentication Port**—The UDP port over which the proxy RADIUS server conducts authentication sessions. If the LEAP Proxy RADIUS server is installed on the same Windows server as Cisco Secure ACS, this port should not be the same port used by Cisco Secure ACS for RADIUS authentication. For more information about the ports used by Cisco Secure ACS for RADIUS, see RADIUS, page 1-7.
- **Timeout (seconds):**—The number of seconds Cisco Secure ACS waits before sending notification to the user that the authentication attempt has timed out.
- **Retries**—The number of authentication attempts Cisco Secure ACS makes before failing over to the secondary proxy RADIUS server.
- **Failback Retry Delay (minutes)**—The number of minutes after which Cisco Secure ACS attempts authentications using a failed primary proxy RADIUS server.

**Note** If both the primary and the secondary servers fail, Cisco Secure ACS alternates between both servers until one responds.

**Step 8** Click **Submit**.

Cisco Secure ACS saves the proxy RADIUS token server database configuration you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 15-4. For more information about configuring user accounts to authenticate using this database, see Chapter 7, “User Management”.



Downloaded from www.Manualslib.com manuals search engine

# Token Server User Databases

Cisco Secure ACS supports the use of token servers for the increased security provided by one-time passwords (OTPs).

This section contains the following topics:


- About Token Servers and Cisco Secure ACS, page 13-78
- RADIUS-Enabled Token Servers, page 13-79
- RSA SecurID Token Servers, page 13-84


## About Token Servers and Cisco Secure ACS

Cisco Secure ACS provides ASCII, PAP, and PEAP(EAP-GTC) authentication using token servers. Other authentication protocols are not supported with token server databases.

**Note** Authentication protocols not supported with token server databases may be supported by another type of external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-10.

Requests from the AAA client are first sent to Cisco Secure ACS. If Cisco Secure ACS has been configured to authenticate against a token server and finds the username, it forwards the authentication request to the token server. If it does not find the username, Cisco Secure ACS checks the database configured to authenticate unknown users. If the request for authentication is passed, the appropriate authorizations are forwarded to the AAA client along with the approved authentication. Cisco Secure ACS then maintains the accounting information.

Cisco Secure ACS acts as a client to the token server. For all token servers except RSA SecurID, Cisco Secure ACS accomplishes this using the RADIUS interface of the token server. For more information about Cisco Secure ACS support of token servers with a RADIUS interface, see RADIUS-Enabled Token Servers, page 13-79.



Downloaded from www.Manualslib.com manuals search engine

For RSA SecurID, Cisco Secure ACS uses an RSA proprietary API. For more information about Cisco Secure ACS support of RSA SecurID token servers, see RSA SecurID Token Servers, page 13-84.

## Token Servers and ISDN

Cisco Secure ACS supports token caching for ISDN terminal adapters and routers. One inconvenience of using token cards for OTP authentication with ISDN is that each B channel requires its own OTP. Therefore, a user must enter at least 2 OTPs, plus any other login passwords, such as those for Windows networking. If the terminal adapter supports the ability to turn on and off the second B channel, users might have to enter many OTPs each time the second B channel comes into service.

Cisco Secure ACS caches the token to help make the OTPs easier for users. This means that if a token card is being used to authenticate a user on the first B channel, a specified period can be set during which the second B channel can come into service without requiring the user to enter another OTP. To lessen the risk of unauthorized access to the second B channel, you can limit the time the second B channel is up. Furthermore, you can configure the second B channel to use the CHAP password specified during the first login to further lessen the chance of a security problem. When the first B channel is dropped, the cached token is erased.

# RADIUS-Enabled Token Servers

This section describes support for token servers that provide a standard RADIUS interface.

This section contains the following topics:

- About RADIUS-Enabled Token Servers, page 13-80
- Token Server RADIUS Authentication Request and Response Contents, page 13-80
- Configuring a RADIUS Token Server External User Database, page 13-81



Downloaded from www.Manualslib.com manuals search engine

## About RADIUS-Enabled Token Servers

Cisco Secure ACS supports token servers using the RADIUS server built into the token server. Rather than using a vendor-proprietary API, Cisco Secure ACS sends standard RADIUS authentication requests to the RADIUS authentication port on the token server. This feature enables Cisco Secure ACS to support any IETF RFC 2865-compliant token server.

You can create multiple instances of RADIUS token servers. For information about configuring Cisco Secure ACS to authenticate users with one of these token servers, see Configuring a RADIUS Token Server External User Database, page 13-81.

Cisco Secure ACS provides a means for specifying a user group assignment in the RADIUS response from the RADIUS-enabled token server. Group specification always takes precedence over group mapping. For more information, see RADIUS-Based Group Specification, page 16-14.

Cisco Secure ACS also supports mapping users authenticated by a RADIUS-enabled token server to a single group. Group mapping only occurs if group specification does not occur. For more information, see Group Mapping by External User Database, page 16-2.

## Token Server RADIUS Authentication Request and Response Contents

When Cisco Secure ACS forwards an authentication request to a RADIUS-enabled token server, the RADIUS authentication request contains the following attributes:

- User-Name (RADIUS attribute 1)
- User-Password (RADIUS attribute 2)
- NAS-IP-Address (RADIUS attribute 4)
- NAS-Port (RADIUS attribute 5)
- NAS-Identifier (RADIUS attribute 32)



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS expects to receive one of the following three responses:

- **access-accept**—No attributes are required; however, the response can indicate the Cisco Secure ACS group to which the user should be assigned. For more information, see RADIUS-Based Group Specification, page 16-14.
- **access-reject**—No attributes required.
- **access-challenge**—Attributes required, per IETF RFC, are as follows:
  - State (RADIUS attribute 24)
  - Reply-Message (RADIUS attribute 18)

## Configuring a RADIUS Token Server External User Database

Use this procedure to configure RADIUS Token Server external user databases.

**Before You Begin**

You should install and configure your RADIUS token server before configuring Cisco Secure ACS to authenticate users with it. For information about installing the RADIUS token server, refer to the documentation included with your token server.

To configure Cisco Secure ACS to authenticate users with a RADIUS Token Sever, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Configuration**.

Cisco Secure ACS lists all possible external user database types.

**Step 3** Click **RADIUS Token Server**.

The Database Configuration Creation table appears. If at least one RADIUS token server configuration exists, the External User Database Configuration table also appears.

**Step 4** If you are creating a configuration, follow these steps:

**a.** Click **Create New Configuration**.

**b.** Type a name for the new configuration for the RADIUS-enabled token server in the box provided, or accept the default name in the box.



Downloaded from www.Manualslib.com manuals search engine

c. Click **Submit**.

Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

**Step 5** Under External User Database Configuration, select the name of the RADIUS-enabled token server you need to configure.

**Note** If only one RADIUS-enabled token server configuration exists, the name of that configuration appears instead of the list. Proceed to Step 6.

**Step 6** Click **Configure**.

**Step 7** In the RADIUS Configuration table, type the required information in the following boxes:

- **Primary Server Name/IP**—The hostname or IP address of the primary RADIUS token server. If you provide the hostname, the hostname must be resolvable by DNS.
- **Secondary Server Name/IP**—The hostname or IP address of the secondary RADIUS token server. If you provide the hostname, the hostname must be resolvable by DNS.
- **Shared Secret**—The shared secret of the RADIUS server. This must be identical to the shared secret with which the RADIUS token server is configured.
- **Authentication Port**—The UDP port over which the RADIUS server conducts authentication sessions. If the RADIUS token server is installed on the same Windows server as Cisco Secure ACS, this port should not be the same port used by Cisco Secure ACS for RADIUS authentication. For more information about the ports used by Cisco Secure ACS for RADIUS, see RADIUS, page 1-7.

**Note** For Cisco Secure ACS to send RADIUS OTP messages to a RADIUS-enabled token server, you must ensure that gateway devices between the RADIUS-enabled token server and Cisco Secure ACS allow communication over the UDP port specified in the Authentication Port box.



Downloaded from www.Manualslib.com manuals search engine

- **Timeout (seconds):**—The number of seconds Cisco Secure ACS waits for a response from the RADIUS token server before retrying the authentication request.
- **Retries**—The number of authentication attempts Cisco Secure ACS makes before failing over to the secondary RADIUS token server.
- **Failback Retry Delay (minutes)**—The number of minutes that Cisco Secure ACS sends authentication requests to the secondary server when the primary server has failed. When this duration is ended, Cisco Secure ACS reverts to sending authentication requests to the primary server.

**Note** If both the primary and the secondary servers fail, Cisco Secure ACS alternates between both servers until one responds.

**Step 8** If you want to support token users performing a shell login to a TACACS+ AAA client, you must configure the options in the TACACS+ Shell Configuration table. Do one of the following:

**a.** If you want Cisco Secure ACS to present a custom prompt for tokens, select **Static (sync and async tokens)**, and then type in the Prompt box the prompt that Cisco Secure ACS will present.

For example, if you type "Enter your PassGo token" in the Prompt box, users receive an "Enter your PassGo token" prompt rather than a password prompt.

**Note** If some tokens submitted to this server are synchronous tokens, you must use the **Static (sync and async tokens)** option.

**b.** If you want Cisco Secure ACS to send the token server a password to trigger a challenge, select **From Token Server (async tokens only)**, and then, in the Password box, type the password that Cisco Secure ACS will forward to the token server.

For example, if the token server requires the string "challengeme" in order to evoke a challenge, you should type "challengeme" in the Password box. Users receive a username prompt and a challenge prompt.

**Tip** Most token servers accept a blank password as the trigger to send a challenge prompt.



Downloaded from www.Manualslib.com manuals search engine

**Note** You should only use the **From Token Server (async tokens only)** option if all tokens submitted to this token server are asynchronous tokens.

**Step 9** Click **Submit**.

Cisco Secure ACS saves the RADIUS token server database configuration you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 15-4. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "User Management".

# RSA SecurID Token Servers

Cisco Secure ACS supports ASCII, PAP, and PEAP(EAP-GTC) authentication for RSA SecurID token servers. Other authentication protocols are not supported with RSA SecurID external user databases.

**Note** Authentication protocols not supported with RSA SecurID databases may be supported by another type of external user database. For more information about authentication protocols and the external database types that support them, see Authentication Protocol-Database Compatibility, page 1-10.

Cisco Secure ACS supports mapping users authenticated by a RSA token server to a single group. For more information, see Group Mapping by External User Database, page 16-2.

Cisco Secure ACS supports PPP (ISDN and async) and Telnet for RSA SecurID token servers. It does so by acting as a token-card client to the RSA SecurID token server. This requires that RSA token-card client software must be installed on the computer running Cisco Secure ACS. The following procedure includes steps required to install the RSA client correctly on the computer running Cisco Secure ACS.



Downloaded from www.Manualslib.com manuals search engine

# Configuring an RSA SecurID Token Server External User Database

Cisco Secure ACS supports the RSA SecurID token server custom interface for authentication of users. You can create only one RSA SecurID configuration within Cisco Secure ACS.

**Before You Begin**

You should install and configure your RSA SecurID token server before configuring Cisco Secure ACS to authenticate users with it. For information about installing the RSA SecurID server, refer to the documentation included with your token server.

Make sure you have the applicable RSA ACE Client.

To configure Cisco Secure ACS to authenticate users with an RSA token server, follow these steps:

**Step 1** Install the RSA client on the computer running Cisco Secure ACS:

a. With a username that has administrative privileges, log in to the computer running Cisco Secure ACS.

b. Run the Setup program of the ACE Client software, following setup instructions provided by RSA.

**Note** Do not restart Windows when installation is complete.

c. Locate the ACE Server data directory, for example, `/sdi/ace/data`.

d. Get the file named `sdconf.rec` and place it in the following Windows directory: `%SystemRoot%\system32`.

For example:

```
\winnt\system32
```

e. Make sure the ACE server hostname is in the Windows local host file:

*\Windows directory*`\system32\drivers\etc\hosts`

f. Restart the computer running Cisco Secure ACS.

g. Verify connectivity by running the Test Authentication function of your ACE client application. You can run this from Control Panel.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** In the navigation bar, click **External User Databases**.

**Step 3** Click **Database Configuration**.

Cisco Secure ACS lists all possible external user database types.

**Step 4** Click **RSA SecurID Token Server**.

If no RSA SecurID token server configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

**Step 5** If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new configuration for the RSA SecurID token server in the box provided, or accept the default name in the box.

c. Click **Submit**.

Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

**Step 6** Click **Configure**.

Cisco Secure ACS displays the name of the token server and the path to the authenticator DLL. This information confirms that Cisco Secure ACS can contact the RSA client. You can add the RSA SecurID external user database to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see About Unknown User Authentication, page 15-4. For more information about configuring user accounts to authenticate using this database, see Chapter 7, "User Management".

# Deleting an External User Database Configuration

If you no longer need a particular external user database configuration, you can delete it from Cisco Secure ACS.

To delete an external user database configuration, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Click **Database Configuration**.

Cisco Secure ACS lists all possible external user database types.

**Step 3** Click the external user database type for which you want to delete a configuration.

The External User Database Configuration table appears.

**Step 4** If a list appears in the External User Database Configuration table, select the configuration you want to delete. Otherwise, proceed to Step 5.

**Step 5** Click **Delete**.

A confirmation dialog box appears.

**Step 6** Click **OK** to confirm that you want to delete the selected external user database configuration.

The external user database configuration you selected is deleted from Cisco Secure ACS.



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

# Network Admission Control

NAC enables you to control the degree of access permitted from computers accessing your network through a AAA client configured to enforce NAC. The basis of NAC is the validation of the posture, or state, of computers on a network. The role of Cisco Secure Access Control Server (ACS) for Windows Server in NAC is to perform posture validation.

This chapter contains the following topics:


- About Network Admission Control, page 14-1
- Implementing Network Admission Control, page 14-5
- NAC Databases, page 14-10
- NAC Policies, page 14-16


## About Network Admission Control

This section contains the following topics:


- NAC AAA Components, page 14-2
- Posture Validation, page 14-3
- Posture Tokens, page 14-4
- Non-Responsive NAC-Client Computers, page 14-5




Downloaded from www.Manualslib.com manuals search engine

# NAC AAA Components

The following list defines the components of the NAC AAA paradigm. Posture Validation, page 14-3, describes the posture validation process in which these components are used.

- **NAC-client computer**—A computer running NAC software, as follows:
  - **NAC client**—The NAC client is the Cisco Trust Agent (CTA) application. CTA collects data directly from the computer and from any NAC-compliant applications installed on the computer. It uses this data to create a set of attributes that contain information about the posture of the computer. These attributes are also called *credentials*. For more information about credentials, see About NAC Credentials and Attributes, page 14-11.
  - **NAC-compliant applications**—Applications that integrate with the NAC client. Examples of such applications are Cisco Security Agent and anti-virus programs from Network Associates, Symantec, or Trend Micro. These applications provide the NAC client with attributes about themselves, such as the version number of a virus definition file.
- **AAA client**—A network access device, such as a router, whose operating system supports NAC.
- **Cisco Secure ACS**—Performs posture validation of the NAC-client computer, using either internal policies, external policies, or both. When external policies are used, Cisco Secure ACS forwards posture validation requests to a NAC server.
- **NAC server**—Performs posture validation of the NAC-client computer when Cisco Secure ACS is configured to use external policies.
- **Remediation server**—Provides support to NAC-client computers needing repairs or updates to comply with network admission requirements.



Downloaded from www.Manualslib.com manuals search engine

# Posture Validation

Cisco Secure ACS determines the posture of a computer by using the credentials received from a NAC-client computer. The following list provides an overview of the steps and systems involved in posture validation. Details about various concepts, such as posture tokens and policies, are provided in topics that follow.

1. The NAC-client computer sends traffic on the network.
2. The NAC-compliant AAA client receives the traffic and initiates an EAP session, forwarding the EAP identity of the NAC-client computer to Cisco Secure ACS.
3. Cisco Secure ACS initiates a PEAP session with the NAC-client computer, so that all NAC communications are encrypted and trusted.
4. The NAC client sends to Cisco Secure ACS a posture validation request, containing credentials from each NAC-compliant application installed on the computer.
5. Using the received credentials, Cisco Secure ACS does the following:
   a. Cisco Secure ACS uses the Unknown User Policy to determine which NAC database to use to perform the posture validation, selecting the first NAC database whose mandatory credential types are satisfied by the credentials in the validation request.

**Note** If the Unknown User Policy cannot find a NAC database whose mandatory credential types are satisfied by the credentials in the validation request, Cisco Secure ACS rejects the request.

   b. Cisco Secure ACS applies all policies associated with the selected NAC database to derive application posture tokens, which are symbols representing the state of the associated application.
   c. Cisco Secure ACS compares all derived application posture tokens and uses the worst token as the system posture token, which symbolizes the overall posture of the NAC-client computer.
   d. Cisco Secure ACS uses the system posture token and group mappings for the selected NAC database to determine which user group contains the authorizations applicable to the NAC-client computer.



Downloaded from www.Manualslib.com manuals search engine

6. Cisco Secure ACS sends the NAC-client computer the system posture token and the results of each policy applied to the posture validation request, and then ends the PEAP session.
7. Cisco Secure ACS sends the AAA client the RADIUS attributes as configured in the mapped user group, including ACLs and attribute-value pairs configured in the Cisco IOS/PIX RADIUS attribute cisco-av-pair.
8. Cisco Secure ACS logs the results of the posture validation request. If the request resulted in a system posture token of Healthy, Cisco Secure ACS logs the results in the Passed Authentications log (if it is enabled). Cisco Secure ACS logs in the Failed Attempts log the result of a posture validation request resulting in a posture token of anything other than Healthy.

The NAC client handles the results of the posture validation request according to its configuration. The AAA client enforces network access as dictated by Cisco Secure ACS in its RADIUS response. By configuring group mapping, you define authorizations and, therefore, network access control, based on the system posture token determined as a result of posture validation.

# Posture Tokens

Posture tokens are symbols that represent the state of a NAC-client computer or a NAC-compliant application installed on the computer. A token associated with the state of the computer is a *system posture token* (SPT). A token associated with the state of a NAC-compliant application is an *application posture token* (APT).

APTs are the result of applying a policy to the credentials received in a posture validation request. Cisco Secure ACS determines the SPT of each request by comparing the APTs from all policies applied to the request. The worst APT becomes the SPT.

There are five predefined, non-configurable posture tokens, used for both SPTs and APTs. Listed in order from best to worst, they are as follows:

- Healthy
- Checkup
- Quarantine
- Infected
- Unknown



Downloaded from www.Manualslib.com manuals search engine

From the perspective of Cisco Secure ACS, the meaning of an SPT is determined by which groups you map each SPT to and how you configure those groups. In other words, the SPTs for each NAC database are associated with configurable network authorizations.

Posture validation requests resulting in an SPT of Healthy are logged in the Passed Authentications log. Posture validation requests resulting in an SPT of anything other than Healthy are logged in the Failed Attempts log.

Aside from being used to determine the SPT, APTs are not meaningful to Cisco Secure ACS, but the NAC client receiving the results of the posture validation can use them based on their meanings to the relevant NAC-compliant application.

## Non-Responsive NAC-Client Computers

NAC-compliant AAA clients can handle NAC for computers that do not respond to attempts to start a posture validation session with CTA. This occurs if CTA is not installed on the computer or is unreachable for other reasons. To account for this scenario, IOS enables you to define a username and password that it uses for authorization requests on behalf of all non-responsive computers.

In Cisco Secure ACS, you must create the corresponding user account and use one of the following features to control network access for non-responsive computers:

- **Downloadable IP ACLs**—You can create a downloadable IP ACL set that limits sessions originating from all non-responsive computers.
- **Network Access Restrictions**—You can create a non-shared network access restriction that disallows any network access for sessions originating from non-responsive computers.
- **Disabled Account**—You can disable the user account used to assign authorization to non-responsive computers, thus disallowing any network access from non-responsive computers.

# Implementing Network Admission Control

This procedure provides steps for implementing NAC support in Cisco Secure ACS, with references to more detailed procedures for each step.



Downloaded from www.Manualslib.com manuals search engine

To implement NAC, follow these steps:

**Step 1** Install a server certificate. Cisco Secure ACS requires a server certificate for NAC because NAC communication with an end-user client is protected by a TLS tunnel. You can use a certificate acquired from a third-party certificate authority (CA) or you can use a self-signed certificate.

For detailed steps about installing a server certificate, see Installing a Cisco Secure ACS Server Certificate, page 10-35. For detailed steps about generating and installing a self-signed certificate, see Generating a Self-Signed Certificate, page 10-49.

**Note** If you use a self-signed certificate, you may need to export the certificate from Cisco Secure ACS and import it as a trusted root CA certificate into local storage on NAC-client computers.

**Step 2** If you want to validate NAC clients with external policies and the following are both true:

- Cisco Secure ACS uses HTTPS to communicate with external NAC servers.
- The external NAC servers use a different CA than the CA that issued the Cisco Secure ACS server certificate installed in Step 1

then you must configure the Certificate Trust List (CTL). For detailed steps, see Editing the Certificate Trust List, page 10-38.

If the CA that issued the server certificates used by the external database servers does not appear on the CTL, you must add the CA. For detailed steps, see Adding a Certificate Authority Certificate, page 10-37.

**Step 3** (Optional) If the Passed Authentications log is not enabled, consider enabling it. Posture validation requests receiving an SPT of Healthy are logged to the Passed Authentications log. You can configure the Passed Authentications log to record useful NAC information, such as posture token-group mapping results. If you enable the Passed Authentications log, be sure to move NAC-related attributes to the Logged Attributes column on the Passed Authentications File Configuration page.

For detailed steps about configuring this type of log, see Configuring a CSV Log, page 11-19.



Downloaded from www.Manualslib.com manuals search engine

**Step 4** Configure the Failed Attempts log to include NAC attributes. Posture validation requests receiving an SPT other than Healthy are logged to the Failed Attempts log. Including NAC attributes in this log can help you debug errors in your NAC implementation. For example, a local policy may return a result that you did not anticipate because of errors in the rules that compose the policy. Using the Failed Attempts log, you can see the contents of the attributes received in the request from the NAC client and sent in the reply to the NAC client.

For detailed steps about configuring this type of log, see Configuring a CSV Log, page 11-19.

**Step 5** On the Global Authentication Setup page, enable NAC by selecting "Enable CNAC" under PEAP.

For detailed steps, see Configuring Authentication Options, page 10-33.

**Step 6** If the AAA clients supporting NAC are not already configured in the Network Configuration section, do so now.

For detailed steps, see Adding a AAA Client, page 4-16.

**Step 7** Select the user groups that you want to use for NAC. You are likely to want a separate user group for each possible SPT; therefore, select five user groups. If possible, choose groups that have not been configured to authorize users. Additionally, consider using groups widely separated from groups used to authorize users. For example, assuming that the lowest numbered groups have been used for user authorization, consider using groups 494 through 499.

**Tip** To avoid confusion between groups intended to authorize users and groups intended to authorize NAC clients, consider renaming the groups with an easily understood name. For example, if you selected group 499 to contain authorizations related to the Unknown SPT, you could rename the group "NAC Unknown". For detailed steps, see Renaming a User Group, page 6-55.

**Step 8** For each NAC-client configuration (and, therefore, each unique set of credential types) that you want to validate, follow these steps:

**a.** Create a NAC database, including configuring mandatory credential types and policies.

For detailed steps, see Configuring a NAC Database, page 14-14.



Downloaded from www.Manualslib.com manuals search engine

b. Create SPT-to-user-group mappings. Each NAC database has its own group mappings.

   For detailed steps, see Configuring NAC Group Mapping, page 16-13.

**Step 9** Configure the Unknown User Policy to include NAC databases. When unknown user processing is enabled, Cisco Secure ACS uses the Unknown User Policy to determine if it has a NAC database whose mandatory credential types are satisfied by the attributes received from the NAC client. Of the NAC databases included in the Selected Databases list on the Configure Unknown User Policy page, Cisco Secure ACS uses the first one whose mandatory credential types are satisfied to process the posture validation request.

For detailed steps, see Configuring the Unknown User Policy, page 15-16.

**Note** You may want to create a default NAC database and place it at the bottom of the Selected Databases list. A default NAC database has no mandatory credential types and therefore can perform posture validation for any request, regardless of the credentials included in the request.

**Step 10** For each SPT, create a downloadable IP ACL set that limits network access appropriately. If you have more than one NAC database and need to control network access differently for the same SPT for each NAC, you must create downloadable IP ACLs per SPT per NAC database. For example, if you have two NAC databases, one for NAI posture validation and one for Symantec posture validation, you may want separate downloadable IP ACLs for a Quarantine SPT, one that allows access only to a Symantec anti-virus server and one that allows access only to a NAI anti-virus server.

For detailed steps, see Adding a Downloadable IP ACL, page 5-10.

**Step 11** For each group to which you have mapped an SPT, follow these steps:

a. Assign the appropriate ACLs to the group. For example, to the group intended to authorize NAI NAC clients whose posture validation returned an Infected SPT, assign the ACL you created to control access of NAI NAC clients whose system posture is Quarantine.

   For detailed steps, see Assigning a Downloadable IP ACL to a Group, page 6-30.



Downloaded from www.Manualslib.com manuals search engine

b. (Optional) If AAA clients participating in NAC are configured to make use of NAC-related attribute-value (AV) pairs in the RADIUS (Cisco IOS/PIX) cisco-av-pair attribute, configure the RADIUS (Cisco IOS/PIX) cisco-av-pair attribute with the applicable AV pairs. NAC-related AV pairs include:

- url-redirect
- posture-token
- status-query-timeout

**Caution** The posture-token AV pair is the only way that Cisco Secure ACS notifies the AAA client of the SPT returned by posture validation. Because you manually configure the posture-token AV pair, errors in configuring posture-token can result in the incorrect SPT being sent to the AAA client or, if the AV pair name is mistyped, the AAA client not receiving the SPT at all.

**Note** The AV pair names above are case sensitive.

For detailed steps about configuring the RADIUS (Cisco IOS/PIX) cisco-av-pair attribute in a group profile, see Configuring Cisco IOS/PIX RADIUS Settings for a User Group, page 6-40. For more information about the RADIUS (Cisco IOS/PIX) cisco-av-pair attribute, see About the cisco-av-pair RADUIS Attribute, page C-7.

Cisco Secure ACS is configured to process posture validation requests, return the results to the NAC client, and send the applicable ACLs to the AAA client.

**Step 12** Create a user account to support NAC in the event of a non-responsive computer. For more information, see Non-Responsive NAC-Client Computers, page 14-5.

Cisco Secure ACS is configured to support NAC of non-responsive computers.



Downloaded from www.Manualslib.com manuals search engine

# NAC Databases

This section contains the following topics:


- About NAC Databases, page 14-10
- About NAC Credentials and Attributes, page 14-11
- NAC Database Configuration Options, page 14-12
- Policy Selection Options, page 14-13
- Configuring a NAC Database, page 14-14


## About NAC Databases

NAC databases validate the posture of a NAC-client computer, using the credentials that the NAC clients sends to Cisco Secure ACS in the posture validation request.

**Tip** Despite the placement of NAC database pages in the External User Databases section of the HTML interface, NAC databases may not involve external databases and Cisco Secure ACS performs no user authentication with a NAC database.

A NAC database consists of the following:

- **Mandatory credential types**—A NAC database has zero or more mandatory credential types. Cisco Secure ACS determines whether to use a NAC database to evaluate a posture validation request by comparing the credentials received in the request to the mandatory credentials types associated with a NAC database. If the request includes each credential type specified, Cisco Secure ACS uses the NAC database to evaluate the request; otherwise, Cisco Secure ACS uses the Unknown User Policy to compare the credentials received to the mandatory credential types of other NAC databases.

  A NAC database without any mandatory credential types is a valid configuration. Cisco Secure ACS considers any posture validation request to satisfy the mandatory credential types of a NAC database that has zero



Downloaded from www.Manualslib.com manuals search engine

mandatory credential types. This design enables you to create a default database so that no posture validation request is rejected due to missing credential types.

- **Credential validation policies**—A NAC database has one or more credential validation policies. When Cisco Secure ACS uses a NAC database to evaluate a posture validation request, it applies each policy associated with the NAC database to the attributes received in the request.

# About NAC Credentials and Attributes

For posture validation, credentials are the sets of attributes sent from the NAC client to Cisco Secure ACS. Also known as inbound attributes, these attributes contain data used during posture validation to determine the posture of the computer. Cisco Secure ACS considers attributes from each NAC-compliant application and from CTA to be different types of credentials.

With local policies, the rules you create use the content of inbound attributes to determine the APT returned by applying the policy. With external policies, Cisco Secure ACS forwards the credential types you specify to the external NAC server. In either case, the contents of inbound attributes provide the information used to determine posture and thus to control network admission for the computer.

Cisco Secure ACS uses NAC attributes in its response to the NAC client. These attributes are known as outbound attributes. For example, APTs and the SPT are sent to the NAC client in attributes.

Credential types are uniquely identified by the combination of two identifiers: vendor ID and application ID. The vendor ID is the number assigned to the vendor in the IANA Assigned Numbers RFC. For example, vendor ID 9 corresponds to Cisco Systems, Inc. Vendors assign numbers to the NAC applications they provide. For example, with Cisco Systems, Inc. applications, application ID 1 corresponds to CTA. In the HTML interface, when you specify result credential types for a local policy, credential types are identified by the names assigned to the vendor and application. For example, the credential type for CTA is Cisco:PA ("PA" refers to "posture agent", another term for CTA). In a posture validation response, Cisco Secure ACS would use the numeric identifiers 9 and 1, which are the identifiers for Cisco and CTA.

Attributes are uniquely identified by the combination of three identifiers: vendor ID, application ID, and attribute ID. For each unique combination of vendor and application, there are set of attributes that each have numbers as well. When



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS communicates with a NAC client, the identifiers are numerical. In the HTML interface, when you define rules for local policies, attributes are identified by the names assigned to vendor, application, and attribute. For example, the CTA attribute for the version of the operating system is Cisco:PA:OS-Version. The data that Cisco Secure ACS receives identifies the attribute with the numeric identifiers 9, 1, and 6, which are the identifiers for Cisco, CTA, and the sixth attribute of CTA.

For more information about attributes, including data types and operators used in rules for local policies, see About Rules, Rule Elements, and Attributes, page 14-19.

# NAC Database Configuration Options

On the Expected Host Configuration page you can configure a NAC database. The options for configuring a NAC database are as follows:

- **Mandatory Credential Types**—Displays the following options:
  - **Credential Types**—Displays the credential types that must be present in a posture validation request in order for Cisco Secure ACS to use the database to evaluate the request. If a request does not contain the mandatory credential types, Cisco Secure ACS will not use the database to evaluate the request.

**Note** The Unknown User Policy uses the mandatory credential types to determine if Cisco Secure ACS can use a given NAC database to evaluate a posture validation request. For more information, see Chapter 15, "Unknown User Policy".

  - **Edit List button**—Enables you to access the Edit Credential Types page for the NAC database.
- **Credential Validation Policies**—Lists the policies Cisco Secure ACS applies to each posture validation request evaluated by the NAC database. This table contains the following options:
  - **Type**—Indicates whether the policy is a local policy or an external policy.



Downloaded from www.Manualslib.com manuals search engine

- **Name**—Displays the policy name as a link. You can click the link to open the applicable policy configuration page, which enables you to view policy details, edit the policy, or delete the policy.
- **Description**—Displays the description associated with the policy. The text displayed in the Description column for a given policy corresponds to the text last saved in the Description box.
- **Local Policies button**—Enables you to go to the Select Local Policies page for the current NAC database. From that page, you can select local policies that the current NAC database uses and you can also access the Local Policy Configuration page to create additional local policies.
- **External Policies button**—Enables you to go to the Select External Policies page for the current NAC database. From that page, you can select external policies that the current NAC database uses and you can also access the External Policy Configuration page to create additional local policies.

# Policy Selection Options

Policy selection pages enable you to specify the policies that Cisco Secure ACS should use to evaluate posture validation requests with the current NAC database. On the Select Local Policies page, you specify the local policies to be used. On the Select External Policies page, you can specify the external policies to be used. The options for selecting policies are as follows:

- **Available Policies**—Lists the policies that Cisco Secure ACS *does not* use to evaluate the posture validation request with this database.
- **Selected Policies**—Lists the policies that Cisco Secure ACS *does* use to evaluate the posture validation request with this database.
- **New Policy button**—Enables you to go to the applicable policy configuration page.



Downloaded from www.Manualslib.com manuals search engine

# Configuring a NAC Database

This procedure describes how you can configure a NAC database.

**Before You Begin**

For descriptions of the options available on the Expected Host Configuration page, see NAC Database Configuration Options, page 14-12.

For descriptions of the options available on the Select Local Policies page and Select Local Policies page, see Policy Selection Options, page 14-13.

To configure a NAC database, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Configuration**.

Cisco Secure ACS displays a list of all possible external user database types.

**Step 3** Click **Network Admission Control**.

If no NAC database exists, only the Database Configuration Creation table appears. Otherwise, in addition to the Database Configuration Creation table, the External User Database Configuration table appears.

**Step 4** If you are creating a configuration, follow these steps:

a. Click **Create New Configuration**.

b. Type a name for the new NAC database in the box provided.

c. Click **Submit**.

Cisco Secure ACS lists the new configuration in the External User Database Configuration table.

**Step 5** Under External User Database Configuration, select the name of the NAC database that you need to configure.

**Note** If only one NAC database exists, the name of that database appears instead of the list. Proceed to the next step.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** Click **Configure**.

**Caution** If you click Delete, the selected NAC database is deleted.

Cisco Secure ACS displays the Expected Host Configuration page for the selected NAC database.

**Step 7** Configure mandatory credential types. To do so, follow these steps:

**a.** Under Mandatory Credential Types, click **Edit List**.

The Edit Credential Types page appears.

**b.** For each credential type that you want to require for validation with this NAC database, select the credential type in the Available Credentials list and click the right arrow (**-->**).

The credential type appears in the Selected Credentials list.

**Tip** To remove a credential type from the Selected Credentials list, select it and click the left arrow (**<--**).

**c.** Click **Submit**.

The Expected Host Configuration page for this NAC database reappears.

The Mandatory Credential Types table lists the selected credential types. Cisco Secure ACS will use this NAC database for posture validation only when the validation request contains attributes for the credential types displayed in the Mandatory Credential Types table.

**Step 8** Select the policies that Cisco Secure ACS must use to validate NAC clients with this NAC database. You can select local policies, external policies, or both. To do so, follow these steps:

**a.** Click either **Local Policies** or **External Policies**, as applicable.

A policy selection page displays Available Policies and Selected Policies lists.



Downloaded from www.Manualslib.com manuals search engine

b. If you need to create a policy, do one of the following, as applicable:

- Click **New Local Policy** and follow the steps in Creating a Local Policy, page 14-25 before continuing this procedure.
- Click **New External Policy** and follow the steps in Creating an External Policy, page 14-32 before continuing this procedure.

c. For each policy that you want to use to validate NAC clients with this NAC database, select the policy in the Available Policies list and click the right arrow (**-->**).

The policy appears in the Selected Policies list.

**Tip** To remove a policy from the Selected Policies list, select it and click the left arrow (**<--**).

d. Click **Submit**.

In the Credential Validation Policies table, the Expected Host Configuration page displays the policies you selected.

e. Repeat a. through d., as needed.

**Step 9** Click **Save Configuration**.

Cisco Secure ACS saves the NAC database you created.

You can add the new NAC database to the Unknown User Policy and you can configure group mapping for the NAC database.

**Note** Until group mapping is established, posture validation with the new NAC database does not control access of the NAC client.

# NAC Policies

Cisco Secure ACS applies to a validation request the policies that you have selected for the NAC database that Cisco Secure ACS uses to evaluate the request.



Downloaded from www.Manualslib.com manuals search engine

Policies are reusable; that is, you can associate a single policy with more than one NAC database. For example, if your NAC implementation requires two NAC databases, one for NAC clients using NAI software and one for NAC clients using Symantec software, you may need to apply the same rules about the operating system of the NAC client regardless of which anti-virus application is installed. You can create a single policy that enforces rules about the operating system and associate it with the Symantec NAC database and the NAI NAC database.

The results of applying a policy are as follows:

- **Result credential type**—The credential type and, therefore, the NAC-compliant application to which the policy evaluation result applies.
- **Token**—One of five predefined tokens that represents the posture of the NAC client and, specifically, the application defined by the result credential type.
- **Action**—An optional text string, sent in the posture validation response to the application defined by the result credential type.

There are two kinds of policies: local and external.

This section contains the following topics:

- Local Policies, page 14-17
- External Policies, page 14-28
- Editing a Policy, page 14-34
- Deleting a Policy, page 14-36

# Local Policies

This section contains the following topics:

- About Local Policies, page 14-18
- About Rules, Rule Elements, and Attributes, page 14-19
- Local Policy Configuration Options, page 14-22
- Rule Configuration Options, page 14-24
- Creating a Local Policy, page 14-25



Downloaded from www.Manualslib.com manuals search engine

# About Local Policies

Local policies consist of one or more rules that you that define in Cisco Secure ACS. When Cisco Secure ACS applies a local policy, it uses the policy rules to evaluate credentials received with the posture validation request. Each rule is associated with an APT, a credential type, and an action. The credential type determines which NAC-compliant application the APT and action are associated with.

Cisco Secure ACS applies each rule in the order they appear on the Policy Configuration page (from top to bottom), resulting in one of the following two possibilities:

- **A configurable rule matches**—When all elements of a rule are satisfied by the credentials received in a posture validation request, the result of applying the policy is the result credential type, APT, and action associated with the rule. Cisco Secure ACS does not evaluate the credentials with any additional rules.
- **No configurable rule matches**—When the attributes included in the posture validation request satisfy no policy rules, Cisco Secure ACS uses the result credential type, application posture token, and action associated with the default rule as the result of the policy.

**Note** Applying a policy to a posture validation request always results in a match, either to one of the configurable rules or to the default rule.

When you specify the order of rules in a policy, determine the likelihood of each rule to be true and then order the rules so that the rule most likely to be true is first and the rule least likely to be true is last. Doing so makes rule processing more efficient; however, determining how likely a rule is to be true can be challenging. For example, one rule may be true for the posture of twice as many NAC clients as a second rule, but posture validation may occur more than twice as often for NAC clients whose posture matches the second rule; therefore, the second rule should be listed first.



Downloaded from www.Manualslib.com manuals search engine

# About Rules, Rule Elements, and Attributes

A rule is a set of one or more rule elements. A rule element is a logical statement consisting of the following three items:

- A posture validation attribute
- An operator
- A value

Cisco Secure ACS uses the operator to compare the contents of an attribute to the value. Each rule element of a rule must be true for the whole rule to be true. In other words, all rule elements of a rule are "anded" together.

This section contains the following topics:

- NAC Attribute Data Types, page 14-19
- Rule Operators, page 14-20

## NAC Attribute Data Types

Posture validation attributes can be one of the following data types:

- **boolean**—The attribute can contain a value of either 1 or 0 (zero). In the HTML interface, when you define a rule element with a boolean attribute, valid input are the words `false` and `true`. Valid operators are = (equal to) and != (not equal to). When a rule element using a boolean attribute is evaluated, `false` corresponds to a value of 0 (zero) and `true` corresponds to 1.

  For example, if a rule element for a boolean attribute requires that the attribute is not equal to `false` and the attribute in a specific posture validation request was 1, Cisco Secure ACS would evaluate the rule element to be true; however, to avoid confusion, you can express the rule element more clearly by requiring that the attribute is equal to `true`.

- **string**—The attribute can contain a string. Valid operators are = (equal to), != (not equal to), contains, starts-with, and regular-expression.
- **integer**—The attribute can contain an integer, including a signed integer. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), >= (greater than or equal to). Valid input in rule elements is an integer between -65535 and 65535.



Downloaded from www.Manualslib.com manuals search engine

- **unsigned integer**—The attribute can contain only an integer without a sign. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), and >= (greater than or equal to). Valid input in rule elements is a whole number between 0 and 4294967295.
- **ipaddr**—The attribute can contain an IPv4 address. Valid operators are = (equal to), != (not equal to), and mask. Valid format in rule elements is dotted decimal format. If the operator is mask, the format is the `mask/IP`. For more information, see Rule Operators, page 14-20.
- **date**—The attribute can contain a date. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), >= (greater than or equal to), and days-since-last-update. Valid format in rule elements:

  *mm*/*dd*/*yyyy*
  *hh*:*mm*:*ss*

- **version**—The attribute can contain an application or data file version. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), and >= (greater than or equal to). Valid format in rule elements:

  *n*.*n*.*n*.*n*

  where each *n* can be an integer from 0 to 65535.
- **octet-array**—The attribute can contain data of arbitrary type and variable length. Valid operators are = (equal to) and != (not equal to). Valid input in rule elements is any hexadecimal number, such as 7E (the hexadecimal equivalent of 126).

## Rule Operators

When you construct a rule on the Rule Configuration page, Cisco Secure ACS only allows you to select an operator that is applicable to the type of attribute you select. For example, if you select the `Cisco:PA:PA-Name` attribute, Cisco Secure ACS permits the use of the `contains` operator in addition to standard mathematical operators; however, if you choose the Cisco:PA:OS-Version attribute, Cisco Secure ACS only permits the use of mathematical operators. For more information about attribute types, see NAC Attribute Data Types, page 14-19.



Downloaded from www.Manualslib.com manuals search engine

The following are the operators that Cisco Secure ACS supports:

- **= (equal to)**—The rule element is true if the value contained in the attribute is exactly equal to the value that you specify.
- **!= (not equal to)**—The rule element is true if the value contained in the attribute does not equal to the value that you specify.

**Tip** Using the != operator can lead to confusion, especially with boolean attributes. For example, if a rule element for a boolean attribute requires that the attribute is not equal to `false` and the attribute in a specific posture validation request was 1, Cisco Secure ACS would evaluate the rule element to be true. To avoid confusion, you can express the rule element more clearly by requiring that the attribute is equal to `true`.

- **> (greater than)**—The rule element is true if the value contained in the attribute is greater than the value that you specify.
- **< (less than)**—The rule element is true if the value contained in the attribute is less than the value that you specify.
- **<= (less than or equal to)**—The rule element is true if the value contained in the attribute is less than or equal to the value that you specify.
- **>= (greater than or equal to)**—The rule element is true if the value contained in the attribute is greater than or equal to the value that you specify.
- **contains**—The rule element is true if the attribute contains a string and if any part of that string matches the string that you specify. For example, using the contains operator and a value of `sc` would match an attribute containing the string `Cisco`, the string `scsi`, or the string `disc`.
- **starts-with**—The rule element is true if the attribute contains a string and if the beginning of that string matches the string that you specify. For example, using the starts-with operator and a value of `Ci` would match an attribute containing the string `Cisco` or the string `Ciena`.
- **regular-expression**—The rule element is true if the attribute contains a string and if the string matches the regular expression that you specify. Cisco Secure ACS supports the following regular expression operators:
  - **^ (caret)**—The ^ operator matches the start of a string. For example `^Ci` would match the string `Cisco` or the string `Ciena`.



Downloaded from www.Manualslib.com manuals search engine

  - **$ (dollar)**—The $ operator matches the end of a string. For example, `co$` would match the string `Cisco` or the string `Tibco`.

- **days-since-last-update**—The rule element is true if the attribute contains a date and if the difference in days between that date and the current date is less than or equal to the number that you specify. For example, in the following rule element:

  ```
  Symantec:AV:DAT-Date days-since-last-update 14
  ```

  the rule element is true for posture validation requests whose Symantec:AV:DAT-Date attribute contain a date that is no more than 14 days in the past.

- **mask**—The rule element is true if the attribute contains an IP address and if that address belongs to the subnet identified by the netmask and IP address that you specify as the rule element value. The format for the rule element value is:

  ```
  mask/IP
  ```

  For example, using the mask operator with a value of `255.255.255.0/192.168.73.8` would match an attribute containing an IP address of 192.168.73.0 to 192.168.73.255. Any mask is permissible and Cisco Secure ACS determines the set of IP addresses matching the value specified using standard subnet masking logic.

## Local Policy Configuration Options

On the Local Policy Configuration page you can specify the rules that make up a policy, including their order. The options for configuring a local policy are as follows:

- **Name**—Specifies the name by which you want to identify the policy. When selecting a policy for a NAC database, you select it by name, and the description is not viewable on the policy selection page; therefore, you should make the name as useful as possible.

**Note** The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the following four characters: [ ] , /



Downloaded from www.Manualslib.com manuals search engine

- **Description**—Specifies a text description of the policy, up to 255 characters. Use the Description box to provide details that you could not convey in the name of the policy. For example, you could describe its purpose or summarize its rules. Because you can apply the same policy to more than one NAC database, a useful description could also help prevent accidental configuration errors when someone modifies a policy without understanding which databases use it.
- **Configurable Rules**—Lists rules that you define in the order in which Cisco Secure ACS uses them to evaluate the posture validation request. Each rule appears as a separate row in the table and is identified by its rule elements, which appear as a blue link. You can order the rules in this table by selecting the option directly to the left of a rule and clicking Up and Down to position it as needed. For more information about the order of rules, see About Local Policies, page 14-18.

  The Configurable Rules table contains the following options:

  - **Result Credential Type**—Specifies a vendor and application. If the rule is true, the Result Credential Type determines the application to which the token in the corresponding Token list is associated. Credential types are listed by the vendor name and application name. For example, CTA appears on the list as `Cisco:PA`. For more information about credential types, see About NAC Credentials and Attributes, page 14-11.
  - **Token**—Specifies a token, specifically, an APT. If the rule is true, the Token list determines the APT associated with the vendor and application selected in the corresponding Result Credential Type list. For more information about tokens, see Posture Tokens, page 14-4.
  - **Action**—Specifies a text message sent to the application indicated by the Result Credential Type list. Use of the text message is determined by the vendor. Some NAC-compliant applications do not implement the use of the Action box.
- **Default Rule**—If no configurable rule is true, the Default Rule table specifies the credential type, token, and action that Cisco Secure ACS uses as the result of applying the policy.



Downloaded from www.Manualslib.com manuals search engine

**Note** Under Default Rule, the meanings of the Result Credential Type list, Token list, and Action box are identical to the options of the same name in the Configurable Rules table, except that the default rule is automatically true, provided that no rule in the Configurable Rules table is true.

## Rule Configuration Options

On the Rule Configuration page you can specify the rule elements that make up a rule. For more information about rules, see About Rules, Rule Elements, and Attributes, page 14-19.

The options for configuring a rule are as follows:

- **Rule Elements Table**—Lists the rule elements that make up the rule. The information displayed in Attribute, Operator, and Value columns for each rule element reflect the settings specified when the rule element was created. For details about the meaning of each column, see the corresponding option description below.

  The Rule Elements Table is limited to displaying 27 characters in the Attribute column and 11 characters in the Value column.

- **Remove button**—Removes the selected rule element from the Rule Elements Table and sets the Attribute, Operator, and Value options to the values in the corresponding columns of the removed rule element. You can also double-click a rule element to remove it from the table.

**Tip** The Remove button enables you to edit a rule element previously added to the table. After you select the rule and click **remove**, you can change the Attribute, Operator, and Value options (described below) and then click **enter** to return the edited rule to the Rule Elements Table.

- **Attribute**—Lists all posture validation attributes that you can use to specify rules. The attributes listed are only those that can be received from a NAC client. Attributes that can only be sent, such as Cisco:PA:System-Posture-Token, cannot be used in a rule and thus never



Downloaded from www.Manualslib.com manuals search engine

appear in the Attribute list. Each attribute is uniquely identified by the vendor name, application name, and attribute name, displayed alphabetically in the following format:

*vendor-name*:*application-name*:*attribute-name*

- **Operator**—Defines the comparison method by which Cisco Secure ACS evaluates whether the rule element is true. The operators available in the Operator list vary depending upon the type of attribute selected from the Attribute list. In addition to common operators, such as >, <, and =, the Operator list supports a few special operators. For more information about special operators, see About Rules, Rule Elements, and Attributes, page 14-19.
- **Value**—Specifies the value to which Cisco Secure ACS compares the contents of the attribute.
- **Enter button**—Adds the rule element defined in the Attribute, Operator, and Value options to the Rule Elements Table.

## Creating a Local Policy

This procedure describes how you can create a local policy.

**Before You Begin**

Although local policies can be selected for more than one NAC database, the page for creating a local policy must be accessed through the configuration pages of a specific NAC database. The NAC database you use to access the Local Policy Configuration page does not limit which NAC databases can select the new local policy.

For descriptions of the options available on the Local Policy Configuration page, see Local Policy Configuration Options, page 14-22.

For descriptions of the options available on the Rule Configuration page, see Rule Configuration Options, page 14-24.

To create a local policy, follow these steps:

**Step 1** If you have not already done so, access the Local Policy Configuration page. To do so, follow these steps:

**a.** In the navigation bar, click **External User Databases**.



Downloaded from www.Manualslib.com manuals search engine

b. Click **Database Configuration > Network Admission Control**.

Cisco Secure ACS displays a list of NAC databases.

c. Select a NAC database from the list of NAC databases and click **Configure**.

**Tip** If there is only one NAC database, no list of databases appears and you can click **Configure**.

The Expected Host Configuration page for the selected NAC database appears. The Credential Validation Policies table lists the policies selected for this NAC database.

d. Under Credential Validation Policies, click **Local Policies**.

The Select Local Policies page appears.

e. Click **New Local Policy**.

The Local Policy Configuration page appears.

**Step 2** In the Name box, type a descriptive name for the policy.

**Step 3** In the Description box, type a useful description of the policy.

**Step 4** Create one or more rules, as needed to define the policy.

For each rule you want to create, follow these steps:

a. Click **New Rule**.

The Edit Rule page appears.

b. For each rule element you want to add, do each of the following:

- Select an attribute.
- Select an operator.
- Type a value.
- Click **enter**.

For more information about attribute types, see NAC Attribute Data Types, page 14-19. For more information about operators, see Rule Operators, page 14-20.

The rule element appears in the Rule Elements table.

c. Verify that the rule elements are configured as intended.



Downloaded from www.Manualslib.com manuals search engine

**Tip** If you want to change a rule element that you have already added to the Rules Elements table, you edit it by selecting the rule element, clicking **remove**, editing its attribute, operator, or value, and clicking **enter** again.

d. Click **Submit**.

The Policy Configuration page appears again. The new rule appears at the bottom of the Configurable Rules table.

**Tip** You can return to the Edit Rule page by clicking the rule.

e. For the new rule, do each of the following:

- Select a result credential type.
- Select a token.
- Type an action.

For more information about tokens, see Posture Tokens, page 14-4.

If the rule matches the posture validation request, Cisco Secure ACS associates with the policy the result credential type, token, and action that you specify.

**Step 5** After you create the rules required to define the policy, order the rules as needed. Cisco Secure ACS applies a policy by attempting to match rules in the order they appear on the Policy Configuration page, from top to bottom. Policy processing stops upon the first successful rule match, so order is important. To move a rule, follow these steps:

a. Select the rule. To do so, click the button to the left of the rule.

b. Click the **Up** or **Down** button as needed until the rule is positioned where you want.

**Step 6** Configure the Default Rule; in the Default Rule table, do each of the following.

- Select a result credential type.
- Select a token.
- Type an action.



Downloaded from www.Manualslib.com manuals search engine

When Cisco Secure ACS applies this policy to a posture validation request and none of the configurable rules match the request, Cisco Secure ACS associates with the policy the default result credential type, token, and action that you specify.

**Step 7** Click **Submit**.

The Select Local Policies page displays the new policy in the Available Policies list.

**Tip** You can add the policy to any NAC database, not just the NAC database you clicked through to reach the Local Policy Configuration page.

**Step 8** If you are in the process of configuring a new NAC database, resume performing the steps in Configuring a NAC Database, page 14-14.

# External Policies

This section contains the following topics:


- About External Policies, page 14-28
- External Policy Configuration Options, page 14-29
- Creating an External Policy, page 14-32


## About External Policies

External policies are policies that define an external NAC server, usually from an anti-virus vendor, and a set of credential types to be forwarded to the external database. You also have the option of defining a secondary external NAC server.

Cisco Secure ACS does not determine the result of applying an external policy; instead, it forwards the selected credentials to the external NAC server and expects to receive the results of the policy evaluation: an APT, a result credential type, and an action.

Each external policy associated with a NAC database must return a result; otherwise, Cisco Secure ACS rejects policy validation requests evaluated with a NAC database whose external policies do not return a result. For example, if



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS evaluates a posture validation request using a NAC database that has 10 local policies and one external policy, but the external NAC servers associated with the external policy are not online, it is irrelevant that the 10 local policies all return SPTs. The failure of the single external policy causes Cisco Secure ACS to reject the posture validation request.

## External Policy Configuration Options

On the External Policy Configuration page you can specify a NAC server (and an optional second NAC server) that Cisco Secure ACS relies upon to apply the policy and you can configure the set of credential types that Cisco Secure ACS forwards. The options for configuring an external policy are as follows:

- **Name**—Specifies the name by which you want to identify the policy. When selecting a policy for a NAC database, you select it by name, and the description is not viewable on the policy selection page; therefore, you should make the name as useful as possible.

  **Note** The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the following four characters: [ ] , /

- **Description**—Specifies a text description of the policy, up to 255 characters. For each NAC database using the policy, the text you type in the Description box appears beside the policy on the Expected Host Configuration page. Use the Description box to provide details that you could not convey in the name of the policy. For example, you could describe its purpose or summarize its rules.

  Because you can apply the same policy to more than one NAC database, a useful description could also help prevent accidental configuration errors when someone modifies a policy without understanding which databases use it.

- **Server Configuration**—You must specify a primary server. You have the option to specify a secondary server for failover operation. For each posture validation request that an external policy is applied to, Cisco Secure ACS attempts to use the first enabled server configuration in the policy that is enabled. If the first enabled server is the primary server and Cisco Secure



Downloaded from www.Manualslib.com manuals search engine

ACS cannot reach the primary server or the primary server fails to respond to the request, Cisco Secure ACS will use the secondary server, if it is configured and enabled.

For the primary and secondary server configurations, each have the following options:

- **URL**—Specifies the HTTP or HTTPS URL for the server. URLs must conform to the following format:

  `[http[s]://]`*host*`[:`*port*`]/`*resource*

  where *host* is the hostname or IP address of the NAC server, *port* is the port number used, and *resource* is the rest of the URL, as required by the NAC server itself. The URL varies depending upon the server vendor and configuration. For the URL required by your NAC server, please refer to your NAC server documentation.

  The default protocol is HTTP. URLs beginning with the hostname are assumed to be using HTTP. To use HTTPS, you must specify the URL beginning with `https://`.

  If the port is omitted, the default port is used. The default port for HTTP is port 80. The default port for HTTPS is port 443.

  If the NAC server hostname is antivirus1, which uses port 8080 to respond to HTTP requests for the service provided policy.asp, a script kept in a web directory called cnac, valid URLs would be:

  ```
  http://antivirus1:8080/cnac/policy.asp
  antivirus1:8080/cnac/policy.asp
  ```

  If the same server used the default HTTP port, valid URLs would be:

  ```
  http://antivirus1/cnac/policy.asp
  http://antivirus1:80/cnac/policy.asp
  antivirus1/cnac/policy.asp
  antivirus1:80/cnac/policy.asp
  ```

  If the same server used HTTPS on the default port, valid URLs would be:

  ```
  https://antivirus1/cnac/policy.asp
  https://antivirus1:443/cnac/policy.asp
  ```

- **Username**—Specifies the username by which Cisco Secure ACS submits forwarded credentials to the server. If the server is not password protected, the values provided in the Username and Password boxes are ignored.



Downloaded from www.Manualslib.com manuals search engine

- **Password**—Specifies the password for the username in the Username box.
- **Timeout (Sec)**—The number of seconds that Cisco Secure ACS waits for a reply from a server after it forwards the credentials.

  If a secondary server is configured, requests to the primary server that timeout are forwarded to the secondary server.

  If no secondary server is configured or if a request to the secondary server also times out, Cisco Secure ACS cannot apply the external policy and the posture validation request is rejected.

  For each posture validation request, Cisco Secure ACS always tries the primary server first, regardless of whether previous requests timed out.
- **Trusted Root CA**—The certificate authority (CA) that issued the server certificate used by the server. If the protocol is HTTPS, Cisco Secure ACS forwards credentials to a server only if the certificate it presents is issued by the CA specified on this list. If Cisco Secure ACS cannot forward the request to the primary or secondary NAC server because the trusted root CAs did not issue the server certificates, the external policy cannot be applied and, therefore, the posture validation request is rejected.

  If the CA that issued a NAC server certificate is not present on the Trusted Root CA list, you must add the CA certificate to Cisco Secure ACS. For more information, see Adding a Certificate Authority Certificate, page 10-37.

**Note** Cisco Secure ACS does not check NAC server certificates against certificate revocation lists, regardless of whether you have configured a CRL issuer for the CA of the NAC server certificate.

**Tip** Be sure you select the correct certificate type for the CA, not just the name of the CA. For example, if the server presents a VeriSign Class 1 Primary CA certificate and VeriSign Class 1 Public Primary CA is selected on the Trusted Root CA list, Cisco Secure ACS does not forward the credentials to the server when HTTPS is in use.



Downloaded from www.Manualslib.com manuals search engine

- **Forwarding Credential Types**—Contains two lists for use in specifying which credential types are forwarded to the external server.
  - **Available Credentials**—Specifies the credential types that *are not* sent to the external server.
  - **Selected Credentials**—Specifies the credential types that *are* sent to the external server.

## Creating an External Policy

This procedure describes how you can create an external policy.

**Before You Begin**

Although external policies can be selected for more than one NAC database, the page for creating an external policy must be accessed through the configuration pages of a specific NAC database. The NAC database you use to access the External Policy Configuration page does not limit which NAC databases can select the new external policy.

For descriptions of the options available on the External Policy Configuration page, see External Policy Configuration Options, page 14-29.

To create an external policy, follow these steps:

**Step 1** If you have not already done so, access the External Policy Configuration page. To do so, follow these steps:

a. In the navigation bar, click **External User Databases**.

b. Click **Database Configuration > Network Admission Control**.

Cisco Secure ACS displays a list of all possible external user database types.

c. Select a NAC database from the list of NAC databases and click **Configure**.

**Tip** If there is only one NAC database, no list of databases appears and you can click **Configure**.

The Expected Host Configuration page for the selected NAC database appears. The Credential Validation Policies table lists the policies selected for this NAC database.



Downloaded from www.Manualslib.com manuals search engine

d. Under Credential Validation Policies, click **External Policies**.

The Select External Policies page appears.

e. Click **New External Policy**.

The External Policy Configuration page appears.

**Step 2** In the **Name** box, type a descriptive name for the policy.

**Step 3** In the **Description** box, type a useful description of the policy.

**Step 4** In the **Primary Server configuration** area, do the following:

a. Select the **Primary Server configuration** check box.

**Note** If you do not select the Primary Server configuration check box, Cisco Secure ACS uses the secondary server configuration. If no secondary server configuration exists or if the secondary server is unreachable, the posture validation request is rejected.

b. Provide configuration details about the primary NAC server. For more information about the boxes and list in this area, see External Policy Configuration Options, page 14-29.

**Step 5** (Optional) In the **Secondary Server configuration** area, do the following:

a. Select the **Secondary Server configuration** check box

b. Provide configuration details about the secondary NAC server. For more information about the boxes and list in this area, see External Policy Configuration Options, page 14-29.

**Step 6** Select the posture validation credential types that Cisco Secure ACS should send to the external NAC server.

For each posture validation credential type that you want Cisco Secure ACS to send to the external NAC server, select the credential type in the Available Credentials list and click the right arrow (**-->**).

The credential type appears in the Selected Credentials list.

**Tip** To remove a credential type from the Selected Credentials list, select it and click the left arrow (**<--**).

**Step 7** Click **Submit**.



Downloaded from www.Manualslib.com manuals search engine

The Select External Policies page displays the new policy in the Available Policies list.

**Tip** You can add the policy to any NAC database, not just the NAC database you clicked through to reach the External Policy Configuration page.

**Step 8** If you are in the process of configuring a NAC database, resume performing the steps in Configuring a NAC Database, page 14-14.

# Editing a Policy

### Before You Begin

A policy can be edited only by accessing it through a NAC database that includes the policy in its Credential Validation Policies table.

To edit a policy, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Configuration** > **Network Admission Control**.

Cisco Secure ACS displays a list of NAC databases.

**Step 3** Select a NAC database from the list of NAC databases and click **Configure**.

**Tip** If there is only one NAC database, no list of databases appears and you can click **Configure**.

The Expected Host Configuration page for the selected NAC database appears. The Credential Validation Policies table lists the policies selected for this NAC database.

**Step 4** Under **Name**, click the name of the policy you want to edit.



Downloaded from www.Manualslib.com manuals search engine

**Tip** If the policy you want to edit does not appear in the Credential Validation Policies table, click **Local Policies** or **External Policies**, as applicable, move the policy you want to edit to the Selected Policies list, and click **Submit**. You can remove the policy from the Credential Validation Policies table when you are done editing it.

The applicable policy configuration page appears.

**Step 5** Edit the policy as needed. Be aware of the following:

- If you change the name of the policy, clicking Submit creates a new policy. Cisco Secure ACS stores the new policy and does not change the configuration of the old policy. The old policy remains on the Credential Validation Policies table of each database that it was on before creating the new policy.

  When you click Submit after changing the policy name, the applicable policy selection page for the NAC database you selected in Step 3. You can modify the policy selection, if desired, and then click **Submit**.

- To edit a local policy rule, in the Configurable Rules table, click the rule name. The Edit Rule page displays the Rule Elements table. Add, modify, or remove rule elements from the rule as needed, and then click **Submit** to return to the Policy Configuration page.

**Step 6** Click **Submit**.

Cisco Secure ACS saves the changes you made to the policy. The Expected Host Configuration page reappears, or if you changed the policy name, a policy selection page appears, enabling you to select the new policy for the NAC database you selected in Step 3.

**Tip** If you added the policy to the NAC database only so that you could edit it, be sure to remove it from the applicable Selected Policies list. To do so, click **Local Policies** or **External Policies**, as applicable, move the policy to the Available Policies list, and click **Submit**.



Downloaded from www.Manualslib.com manuals search engine

# Deleting a Policy

### Before You Begin

A policy can be deleted only by accessing it through a NAC database that includes the policy in its Credential Validation Policies table.

To delete a policy, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Configuration > Network Admission Control**.

Cisco Secure ACS displays a list of all possible external user database types.

**Step 3** Select a NAC database from the list of NAC databases and click **Configure**.

**Tip** If there is only one NAC database, no list of databases appears and you can click **Configure**.

The Expected Host Configuration page for the selected NAC database appears. The Credential Validation Policies table lists the policies selected for this NAC database.

**Step 4** Under **Name**, click the name of the policy you want to delete.

**Tip** If the policy you want to delete does not appear in the Credential Validation Policies table, click **Local Policies** or **External Policies**, as applicable, move the policy you want to delete to the Selected Policies list, and click **Submit**. After you delete the policy, it will no longer appear in the Credential Validation Policies table for this NAC database and will no longer appear on a policy selection page.

The applicable policy configuration page appears.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** Click **Delete Policy**.

**Step 6** Click **Submit**.

Cisco Secure ACS deletes the policy. The Expected Host Configuration page reappears and the Credential Validation Policies table no longer lists the deleted policy. All NAC databases that were configured to use the policy no longer include the deleted policy.



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

# Unknown User Policy

After you have configured at least one database in the External User Databases section of the HTML interface of Cisco Secure Access Control Server (ACS) for Windows Server, you can decide how to implement other Cisco Secure ACS features related to authentication and posture validation. These features are the Unknown User Policy and user group mapping.

This chapter addresses the Unknown User Policy feature, found in the External User Databases section of the Cisco Secure ACS HTML interface.

For information about user group mapping, see Chapter 16, "User Group Mapping and Specification".

For information about databases supported by Cisco Secure ACS and how to configure databases in the HTML interface, see Chapter 13, "User Databases".

This chapter contains the following topics:


- Known, Unknown, and Discovered Users, page 15-2
- Authentication and Unknown Users, page 15-4
  - About Unknown User Authentication, page 15-4
  - General Authentication of Unknown Users, page 15-5
  - Windows Authentication of Unknown Users, page 15-6
  - Performance of Unknown User Authentication, page 15-8




Downloaded from www.Manualslib.com manuals search engine

- Posture Validation and the Unknown User Policy, page 15-10
  - NAC and the Unknown User Policy, page 15-10
  - Posture Validation Use of the Unknown User Policy, page 15-11
  - Required Use for Posture Validation, page 15-12
- Authorization of Unknown Users, page 15-13
- Unknown User Policy Options, page 15-13
- Database Search Order, page 15-14
- Configuring the Unknown User Policy, page 15-16
- Disabling Unknown User Authentication, page 15-17


# Known, Unknown, and Discovered Users

The Unknown User Policy feature provides different means of handling authentication or posture validation requests, depending upon the type of user requesting AAA services. There are three types of users. Their significance varies depending on whether the service requested is authentication or posture validation:

- **Known Users**—Users explicitly added, either manually or automatically, to the CiscoSecure user database. These are users added by an administrator using the HTML interface, by the RDBMS Synchronization feature, by the Database Replication feature, or by the CSUtil.exe utility. For more information about CSUtil.exe, see Appendix D, "CSUtil Database Utility". Cisco Secure ACS handles authentication and posture validation requests for known users as follows:
  - **Authentication**—Cisco Secure ACS attempts to authenticate a known user with the single user database that the user is associated with. If the user database is the CiscoSecure user database and the user does not represent a Voice-over-IP (VoIP) user account, a password is required for the user. If the user database is an external user database or if the user represents a VoIP user account, Cisco Secure ACS does not have to store a user password in the CiscoSecure user database.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS does not support failover authentication. If authentication fails with the database that the user is associated with, Cisco Secure ACS uses no other means to authenticate the user and Cisco Secure ACS informs the AAA client of the authentication failure.

  - **Posture validation**—Cisco Secure ACS always uses the Unknown User Policy to determine which Network Admission Control (NAC) database to use for a posture validation request. For more information, see Posture Validation and the Unknown User Policy, page 15-10.

- **Unknown Users**—Users who do not have a user account in the CiscoSecure user database. This either means that the user has not received authentication or posture validation services from Cisco Secure ACS or that the user account was deleted. Cisco Secure ACS handles authentication and posture validation requests for unknown users as specified by your configuration of the Unknown User Policy.

  - **Authentication**—For details about unknown user authentication, see General Authentication of Unknown Users, page 15-5.

  - **Posture validation**—Cisco Secure ACS always uses the Unknown User Policy to determine which NAC database to use for a posture validation request. For more information, see Posture Validation and the Unknown User Policy, page 15-10.

- **Discovered Users**—Users whose accounts Cisco Secure ACS created in the CiscoSecure user database after successful authentication or posture validation using the Unknown User Policy. All discovered users were unknown users. When Cisco Secure ACS creates a discovered user, the user account contains only the username, a Password Authentication list setting that reflects the database that provided authentication or posture validation service for the user, and a "Group to which the user is assigned" list setting of Mapped By External Authenticator, which enables group mapping. Using the Cisco Secure ACS HTML interface or RDBMS Synchronization, you can further configure the user account as needed. For example, after a discovered user is created in Cisco Secure ACS, you can assign user-specific network access restrictions to the discovered user.

**Note** Cisco Secure ACS does not import credentials (such as passwords, certificates, or NAC credential types) for a discovered user.



Downloaded from www.Manualslib.com manuals search engine

- **Authentication**—The authentication process for discovered users is identical to the authentication process for known users who are authenticated with external user databases and whose Cisco Secure ACS group membership is determined by group mapping.
- **Posture Validation**—Cisco Secure ACS always uses the Unknown User Policy to determine which NAC database to use for a posture validation request. For more information, see Posture Validation and the Unknown User Policy, page 15-10.

**Note** We recommend removing a username from a database when the privileges associated with that username are no longer required. For more information about deleting a user account, see Deleting a User Account, page 7-57.

# Authentication and Unknown Users

This section provides information about using the Unknown User Policy with authentication. For information about using the Unknown User Policy with NAC, see Posture Validation and the Unknown User Policy, page 15-10.

This section contains the following topics:


- About Unknown User Authentication, page 15-4
- General Authentication of Unknown Users, page 15-5
- Windows Authentication of Unknown Users, page 15-6
- Performance of Unknown User Authentication, page 15-8


## About Unknown User Authentication

The Unknown User Policy is a form of authentication forwarding. In essence, this feature is an extra step in the authentication process. In this additional step, if the username does not exist in the CiscoSecure user database, Cisco Secure ACS forwards the authentication request of an incoming username and password to external databases with which it is configured to communicate and which support the authentication protocol used in the authentication request.



Downloaded from www.Manualslib.com manuals search engine

The Unknown User Policy enables Cisco Secure ACS to use a variety of external databases to attempt authentication of unknown users. This feature provides the foundation for a basic single sign-on capability through Cisco Secure ACS. Because the incoming authentication requests are handled by external user databases, there is no need for you to maintain within Cisco Secure ACS the credentials of users, such as passwords. This provides two advantages:

- Eliminates the necessity of entering every user multiple times.
- Prevents data-entry errors inherent to manual procedures.

# General Authentication of Unknown Users

If you have configured the Unknown User Policy in Cisco Secure ACS, Cisco Secure ACS attempts to authenticate unknown users as follows:

1. Cisco Secure ACS checks its internal user database. If the user exists in the CiscoSecure user database (that is, is a known or discovered user), Cisco Secure ACS tries to authenticate the user with the authentication protocol of the request and the database specified in the user account. Authentication either passes or fails.
2. If the user does not exist in the CiscoSecure user database (that is, is an unknown user), Cisco Secure ACS tries each external user database that supports the authentication protocol of the request, in the order specified in the Selected Databases list. If authentication with one of the external user databases passes, Cisco Secure ACS automatically adds the user to the CiscoSecure user database, with a pointer to use the external user database that succeeded on this authentication attempt. Users added by unknown user authentication are flagged as such within the CiscoSecure user database and are called discovered users.

   The next time the discovered user tries to authenticate, Cisco Secure ACS authenticates the user against the database that was successful the first time. Discovered users are treated the same as known users.
3. If the unknown user fails authentication with all configured external databases, the user is not added to the CiscoSecure user database and the authentication fails.

The scenario given above is handled differently if the user accounts with identical usernames exist in separate Windows domains. For more information, see Windows Authentication of Unknown Users, page 15-6.



Downloaded from www.Manualslib.com manuals search engine

**Note** Because usernames in the CiscoSecure user database must be unique, Cisco Secure ACS supports a single instance of any given username across all databases that it is configured to use. For example, assume every external user database contains a user account with the username John. Each account is for a different user, but they each, coincidentally, have the same username. After the first John attempts to access the network and has authenticated through the unknown user process, Cisco Secure ACS retains a discovered user account for that John and only that John. Now, Cisco Secure ACS tries to authenticate subsequent attempts by any user named John using the same external user database that originally authenticated John. Assuming their passwords are different than the password for the John who authenticated first, the other Johns are unable to access the network.

# Windows Authentication of Unknown Users

Because there can be multiple occurrences of the same username across the trusted Windows domains against which Cisco Secure ACS authenticates users, Cisco Secure ACS treats authentication with a Windows user database as a special case.

To perform authentication, Cisco Secure ACS communicates with the Windows operating system of the computer running Cisco Secure ACS. Windows uses its built-in facilities to forward the authentication requests to the appropriate domain controller.

This section contains the following topics:


- Domain-Qualified Unknown Windows Users, page 15-6
- Windows Authentication with Domain Qualification, page 15-7
- Multiple User Account Creation, page 15-8


## Domain-Qualified Unknown Windows Users

When a domain name is supplied as part of a authentication request, Cisco Secure ACS detects that a domain name was supplied and tries the authentication credentials against the specified domain. The dial-up networking clients provided



Downloaded from www.Manualslib.com manuals search engine

with various Windows versions differ in the method by which users can specify their domains. For more information, see Windows Dial-up Networking Clients, page 13-10.

Using a domain-qualified username allows Cisco Secure ACS to differentiate a user from multiple instances of the same username in different domains. For unknown users who provide domain-qualified usernames and who are authenticated by a Windows user database, Cisco Secure ACS creates their user accounts in the CiscoSecure user database in the form *DOMAIN\username*. The combination of username and domain makes the user unique in the Cisco Secure ACS database.

For more information about domain-qualified usernames and Windows authentication, see Usernames and Windows Authentication, page 13-11.

## Windows Authentication with Domain Qualification

If the username is non-domain qualified or is in UPN format, the Windows operating system of the computer running Cisco Secure ACS follows a more complex authentication order, which Cisco Secure ACS cannot control. Though the order of resources used can differ, when searching for a non-domain qualified username or UPN username, Windows usually follows the order in the list below:

1. The local domain controller.
2. The domain controllers in any trusted domains, in an order determined by Windows.
3. If Cisco Secure ACS runs on a member server, the local accounts database.

Windows attempts to authenticate the user with the first account it finds whose username matches the one passed to Windows by Cisco Secure ACS. Whether authentication fails or succeeds, Windows does not search for other accounts with the same username; therefore, Windows can fail to authenticate a user who supplies valid credentials because Windows may check the supplied credentials against the wrong account that coincidentally has an identical username.

You can circumvent this difficulty by using the Domain List in the Cisco Secure ACS configuration for the Windows user database. If you have configured the Domain List with a list of trusted domains, Cisco Secure ACS submits the username and password to each domain in the list, using a domain-qualified format, until Cisco Secure ACS successfully authenticates the user or until Cisco Secure ACS has tried each domain listed in the Domain List and fails the authentication.



Downloaded from www.Manualslib.com manuals search engine

**Note** If your network has multiple occurrences of a username across domains (for example, every domain has a user called Administrator) or if users do not provide their domains as part of their authentication credentials, be sure to configure the Domain List for the Windows user database in the External User Databases section. If not, only the user whose account Windows happens to check first authenticates successfully. The Domain List is the only way that Cisco Secure ACS controls the order in which Windows checks domains. The most reliable method of supporting multiple instances of a username across domains is to require users to supply their domain memberships as part of the authentication request. For more information about the effects of using the Domain List, see Non-domain-qualified Usernames, page 13-13.

## Multiple User Account Creation

Unknown user authentication can create more than one user account for the same user. For example, if a user provides a domain-qualified username and successfully authenticates, Cisco Secure ACS creates an account in the format *DOMAIN\username*. If the same user successfully authenticates without prefixing the domain name to the username, Cisco Secure ACS creates an account in the format *username*. If the same user also authenticates with a UPN version of the username, such as username@example.com, Cisco Secure ACS creates a third account.

If, to assign authorizations, you rely on groups rather than individual user settings, all accounts that authenticate using the same Windows user account should receive the same privileges. Regardless of whether the user prefixes the domain name, group mapping will assign the user to the same Cisco Secure ACS user group, because both Cisco Secure ACS user accounts correspond to a single Windows user account.

# Performance of Unknown User Authentication

Processing authentication requests for unknown users requires slightly more time than does processing authentication requests for known users. This small delay may require additional timeout configuration on the AAA clients through which unknown users may attempt to access your network.



Downloaded from www.Manualslib.com manuals search engine

## Added Authentication Latency

Adding external user databases against which to authenticate unknown users can significantly increase the time needed for each individual authentication. At best, the time needed for each authentication is the time taken by the external user database to authenticate, plus some time for Cisco Secure ACS processing. In some circumstances (for example, when using a Windows user database), the extra latency introduced by an external user database can be as much as tens of seconds. If you have configured the Unknown User Policy to include multiple databases in unknown user authentication, the latency your AAA client timeout values must account for is the sum of the time taken for each external user database to respond to an authentication request of an unknown user, plus the time taken for Cisco Secure ACS processing.

You can reduce the effect of this added latency by setting the order of databases. If you are using an authentication protocol that is particularly time sensitive, such as PEAP, we recommend configuring unknown user authentication to attempt authentication first with the database most likely to contain unknown users using the time-sensitive protocol. For more information, see Database Search Order, page 15-14.

## Authentication Timeout Value on AAA clients

Be sure to increase the AAA client timeout to accommodate the longer authentication time required for Cisco Secure ACS to pass the authentication request to the external user databases used by unknown user authentication. If the AAA client timeout value is not set high enough to account for the delay required by unknown user authentication, the AAA client times out the request and every unknown user authentication fails.

In Cisco IOS, the default AAA client timeout value is five seconds. If you have Cisco Secure ACS configured to search through several databases or if your databases are slow to respond to authentication requests, consider increasing the timeout values on AAA clients. For more information about authentication timeout values in IOS, refer to your Cisco IOS documentation.



Downloaded from www.Manualslib.com manuals search engine

# Posture Validation and the Unknown User Policy

This section contains the following topics:


- NAC and the Unknown User Policy, page 15-10
- Posture Validation Use of the Unknown User Policy, page 15-11
- Required Use for Posture Validation, page 15-12


## NAC and the Unknown User Policy

For posture validation requests, the Unknown User Policy automates the association of users to a NAC database that applies to the posture validation request. This occurs regardless of user type; however, if the username sent in the PEAP EAP-Identity field from the NAC client is unknown, Cisco Secure ACS also creates the user account in the CiscoSecure user database.

The value sent in the PEAP EAP-Identity field is determined by the NAC client, which is Cisco Trust Agent (CTA); therefore, Cisco Secure ACS is not in control of the username associated with a posture validation request. CTA sends in the EAP-Identity field a string in the following format:

*hostname*:*username*

where *hostname* is the name of the NAC-client computer and *username* identifies the user logged into the NAC-client computer at the time that CTA sends the posture validation request. For example, while the user cyril.yang is logged into the computer named yang-laptop01, posture validation requests received by Cisco Secure ACS contain the string yang-laptop01:cyril.yang in the EAP-Identity field. As a result of the behavior of the Unknown User Policy, Cisco Secure ACS creates a user account named yang-laptop01:cyril.yang.

Because the username is part of the EAP-Identity field value in posture validation requests, Cisco Secure ACS can create multiple user accounts for the same NAC client. Continuing the example of the computer named yang-laptop01, if the user david.fry is logged into the computer at the time of a subsequent posture validation request, the EAP-Identity field contains the string yang-laptop01:david.fry and Cisco Secure ACS creates a user account named yang-laptop01:david.fry.



Downloaded from www.Manualslib.com manuals search engine

Creating different user accounts for the same NAC-client computer enables you to determine from Cisco Secure ACS logs who was logged into a NAC-client computer during posture validation. Because the NAC-compliant applications running on a computer can differ depending upon who is logged into the computer, knowing who is logged in helps you troubleshoot posture validation issues.

Using the Unknown User Policy for posture validation requests provides these advantages:

- Creates user accounts for NAC clients automatically, thereby preventing data-entry errors inherent to adding user accounts manually, such as misspelling the username.
- Supports changes to your NAC implementation by applying the Unknown User Policy to all posture validation requests, regardless of user type.
- Supports the use of a default NAC database, which has no mandatory credential types and therefore applies to all posture validation requests that no other NAC databases can process.

# Posture Validation Use of the Unknown User Policy

If you configured the Unknown User Policy in Cisco Secure ACS, Cisco Secure ACS uses the Selected Databases list of the Unknown User Policy to find a NAC database that can support the posture validation request. A NAC database can perform posture validation only for requests whose credentials satisfy the mandatory credential types of that database. In addition, because you can create a NAC database that has no mandatory credential types, you can use such a database as a default for posture validation requests that cannot be processed by any other NAC database added to your Unknown User Policy.

Because posture validation requests can be processed by one and only one NAC database, Cisco Secure ACS associates the request with the first NAC database in the Selected Databases list whose mandatory credential types are satisfied by the credentials included in the posture validation request. Regardless of the results of posture validation, Cisco Secure ACS never attempts posture validation with subsequent databases in the Selected Databases list. Satisfying the mandatory credential types is the sole criterion used to determine whether a posture validation request is associated with a NAC database. For more information about the order of NAC databases in the Selected Databases list, see Database Search Order, page 15-14.



Downloaded from www.Manualslib.com manuals search engine

**Note** If the credentials included in a posture validation request do not satisfy any NAC databases in the Selected Databases list, Cisco Secure ACS rejects the posture validation request.

For more information about NAC databases, including information about mandatory credential types, see Chapter 14, "Network Admission Control".

# Required Use for Posture Validation

Use of the Unknown User Policy is required for posture validation. With every posture validation request, regardless of the user type, Cisco Secure ACS uses the Unknown User Policy to determine which NAC database is to process the request. This behavior supports changes to the configuration of NAC-client computers, especially when additional NAC-compliant applications have been installed on the computers. Consider the following scenario:

1. A NAC-client computer is added to the network. This computer has CTA installed with no NAC-compliant applications.
2. When Cisco Secure ACS performs posture validation for the new computer, it uses a NAC database that only requires the credentials of CTA. Cisco Secure ACS creates a user account corresponding to the NAC-client computer.
3. A NAC-compliant application is added to the computer, such as Cisco Security Agent (CSA).

The mandatory credential types of the NAC database first used with the computer are still satisfied by the credentials in posture validation requests from it; however, to evaluate the posture of the computer using CSA credentials in addition to CTA credentials, you want a NAC database whose mandatory credentials types include CTA and CSA credentials. By ordering NAC databases carefully on the Selected Databases list, you can ensure that each posture validation request is handled by a NAC database with the most restrictive mandatory credential types and, therefore, the most applicable policies.



Downloaded from www.Manualslib.com manuals search engine

# Authorization of Unknown Users

Although the Unknown User Policy allows authentication and posture validation requests to be processed by databases configured in the External User Database section, Cisco Secure ACS is responsible for all authorizations sent to AAA clients and end-user clients. Posture validation and unknown user authentication work with Cisco Secure ACS user group mapping features to assign unknown users to user groups you have already configured and, therefore, to assign authorization to all NAC clients and to unknown users who pass authentication. For more information, see Chapter 16, "User Group Mapping and Specification".

# Unknown User Policy Options

On the Configure Unknown User Policy page you can specify what Cisco Secure ACS does for posture validation and unknown user authentication. The options for configuring the Unknown User Policy are as follows:

- **Fail the attempt**—Disables unknown user authentication; therefore, Cisco Secure ACS rejects authentication requests for users not found in the CiscoSecure user database. Selecting this option excludes the use of the "Check the following external user databases" option.

  **Note** The "Fail the attempt" option does not apply to posture validation requests. For every posture validation request, Cisco Secure ACS always applies the Unknown User Policy.

- **Check the following external user databases**—Enables unknown user authentication; therefore, Cisco Secure ACS uses the databases in the Selected Databases list to provide unknown user authentication.

  **Note** For authentication requests, Cisco Secure ACS applies the Unknown User Policy to unknown users only. Cisco Secure ACS does not support fallback to unknown user authentication when known or discovered users fail authentication.

  Selecting this option excludes the use of the "Fail the attempt" option.



Downloaded from www.Manualslib.com manuals search engine

- **External Databases**—Of the databases that you have configured in the External User Databases section, lists the databases that Cisco Secure ACS does *not* use during posture validation or unknown user authentication.
- **Selected Databases**—Of the databases that you have configured in the External User Databases section, lists the databases that Cisco Secure ACS *does* use during posture validation and unknown user authentication. Cisco Secure ACS attempts the requested service—authentication or posture validation—using the selected databases one at a time in the order specified. For more information about the significance of the order of selected databases, see Database Search Order, page 15-14.

For detailed steps for configuring your Unknown User Policy, see Configuring the Unknown User Policy, page 15-16

# Database Search Order

You can configure the order in which Cisco Secure ACS checks the selected databases when Cisco Secure ACS attempts posture validation and unknown authentication. The following processes reveal why database order in the Selected Databases list is significant:

- **Authentication**—The Unknown User Policy supports unknown user authentication using the following logic:
  a. Find the next user database in the Selected Databases list that supports the authentication protocol of the request. If there are no user databases in the list that support the authentication protocol of the request, stop unknown user authentication and deny network access to the user.
  b. Send the authentication request to the database found in Step 1.
  c. If the database responds with an “authentication succeeded” message, create the discovered user account, perform group mapping, and grant the user access to the network.
  d. If the database responds with an “authentication failed” message or does not respond and other databases are listed below the current database, return to Step 1.
  e. If there are no additional databases below the current database, deny network access to the user.



Downloaded from www.Manualslib.com manuals search engine

- **Posture validation**—The Unknown User Policy supports all posture validation requests using the following logic:
  a. Of the NAC database in the Selected Databases list, find the first database whose mandatory credential types are satisfied by the credentials received in the posture validation request. If the credentials in the request do not match the mandatory credentials of any database in the list, reject the posture validation request.
  b. Use the NAC database found in Step 1 to perform posture validation for the NAC client.
  c. If Cisco Secure ACS does not have a user profile matching the name provided in the PEAP EAP-Identity field of the posture validation request, create the discovered user account, using the value from the EAP-Identity field as the username. For more information about the effects of using the EAP-Identity field for the username, see NAC and the Unknown User Policy, page 15-10.
  d. Perform group mapping and apply the authorizations specified in the mapped group to the NAC client.

When you specify the order of databases in the Selected Databases list, we recommend placing as near to the top of the list as possible databases that:

- Process the most requests.
- Process requests that are associated with particularly time-sensitive AAA clients or authentication protocols.
- Require the most restrictive mandatory credential types (applies to NAC databases only).

As a user authentication example, if wireless LAN users access your network with PEAP, arrange the databases in the Selected Databases list so that unknown user authentication takes less than the timeout value specified on the Cisco Aironet Access Point.

As a posture validation example, if some NAC clients send more credential types in their posture validation requests than other NAC clients, place higher on the Selected Databases list the NAC databases with the more mandatory credential types; otherwise, Cisco Secure ACS may use a NAC database whose policies do not evaluate client posture using the additional credential types sent by the NAC client.



Downloaded from www.Manualslib.com manuals search engine

**Tip** If you create a default NAC database, that is, a NAC database with no mandatory credential types, be sure you list it below all other NAC databases.

# Configuring the Unknown User Policy

Use this procedure to configure your Unknown User Policy.

**Before You Begin**

For information about the Configure the Unknown User Policy page, see Unknown User Policy Options, page 15-13.

To specify how Cisco Secure ACS processes unknown users, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**, and then click **Unknown User Policy**.

**Step 2** To deny unknown user authentication requests, select the **Fail the attempt** option.

**Note** Selecting the **Fail the attempt** option does not affect posture validation requests. Cisco Secure ACS always uses the Unknown User Policies for posture validation.

**Step 3** To allow unknown user authentication, enable the Unknown User Policy. To do so, follow these steps:

a. Select the **Check the following external user databases** option.

b. For each database that you want Cisco Secure ACS to use for posture validation or unknown user authentication, select the database in the External Databases list and click **-->** (right arrow button) to move it to the Selected Databases list. To remove a database from the Selected Databases list, select the database, and then click **<--** (left arrow button) to move it back to the External Databases list.

c. To assign the database search order, select a database from the Selected Databases list and click **Up** or **Down** to move it into the position you want.



Downloaded from www.Manualslib.com manuals search engine

**Note** For more information about the significance of database order, see Database Search Order, page 15-14.

**Step 4** Click **Submit**.

Cisco Secure ACS saves and implements the Unknown User Policy configuration you created. Cisco Secure ACS processes posture validation requests and unknown user authentication requests using the databases in the order listed in the Selected Databases list.

# Disabling Unknown User Authentication

You can configure Cisco Secure ACS so that it does not provide authentication service to users who are not in the CiscoSecure user database.

**Note** This procedure does not affect posture validation. For more information, see Posture Validation and the Unknown User Policy, page 15-10.

To turn off unknown user authentication, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**, and then click **Unknown User Policy**.

**Step 2** Select the **Fail the attempt** option.

**Step 3** Click **Submit**.

Unknown user authentication is halted. Cisco Secure ACS does not allow unknown users to authenticate with external user databases.



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

CHAPTER 16

# User Group Mapping and Specification

This chapter provides information about group mapping and specification. Cisco Secure Access Control Server (ACS) for Windows Server uses these features to assign users authenticated by an external user database to a single Cisco Secure ACS group.

This chapter contains the following topics:


- About User Group Mapping and Specification, page 16-1
- Group Mapping by External User Database, page 16-2
- Group Mapping by Group Set Membership, page 16-4
- NAC Group Mapping, page 16-13
- RADIUS-Based Group Specification, page 16-14


## About User Group Mapping and Specification

The Database Group Mapping feature in the External User Databases section enables you to associate unknown users with a Cisco Secure ACS group for assigning authorization profiles. For external user databases from which Cisco Secure ACS can derive group information, you can associate the group memberships defined for the users in the external user database to specific Cisco Secure ACS groups. For Windows user databases, group mapping is further




Downloaded from www.Manualslib.com manuals search engine

specified by domain, because each domain maintains its own user database. For Novell NDS user databases, group mapping is further specified by trees, because Cisco Secure ACS supports multiple trees in a single Novell NDS user database.

In addition to the Database Group Mapping feature, for some database types, Cisco Secure ACS supports RADIUS-based group specification.

# Group Mapping by External User Database

You can map an external database to a Cisco Secure ACS group. Unknown users who authenticate using the specified database automatically belong to, and inherit the authorizations of, the group. For example, you could configure Cisco Secure ACS so that all unknown users who authenticate with a certain token server database belong to a group called Telecommuters. You could then assign a group setup that is appropriate for users who are working away from home, such as MaxSessions=1. Or you could configure restricted hours for other groups, but give unrestricted access to Telecommuters group members.

While you can configure Cisco Secure ACS to map all unknown users found in any external user database type to a single Cisco Secure ACS group, the following external user database types are the external user database types whose users you can only map to a single Cisco Secure ACS group:

- ODBC
- LEAP Proxy RADIUS server
- RADIUS token server
- RSA SecurID token server

For a subset of the external user database types listed above, group mapping by external database type is overridden on a user-by-user basis when the external user database specifies a Cisco Secure ACS group with its authentication response. Cisco Secure ACS supports specification of group membership for the following external user database types:

- LEAP Proxy RADIUS server
- RADIUS token server

For more information about specifying group membership for users authenticated with one of these database types, see RADIUS-Based Group Specification, page 16-14.



Downloaded from www.Manualslib.com manuals search engine

Additionally, users authenticated by an ODBC external user database can also be assigned to a specified Cisco Secure ACS group. Group specification by ODBC database authentication overrides group mapping. For more information about specifying group membership for users authenticated with an ODBC database, see ODBC Database, page 13-55.

# Creating a Cisco Secure ACS Group Mapping for a Token Server, ODBC Database, or LEAP Proxy RADIUS Server Database

To set or change a token server, ODBC, or LEAP Proxy RADIUS Server database group mapping, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Group Mappings**.

**Step 3** Click the name of the token server, LEAP Proxy RADIUS Server, or ODBC database configuration for which you want to configure a group mapping.

The Define Group Mapping table appears.

**Step 4** From the **Select a default group for** *database* list, click the group to which users authenticated with this database should be assigned.

**Tip** The **Select a default group for** *database* list displays the number of users assigned to each group.

**Step 5** Click **Submit**.

Cisco Secure ACS assigns unknown and discovered users authenticated by the external database type you selected in Step 3 to the Cisco Secure ACS group selected in Step 4. For users authenticated by an ODBC, RADIUS token server, or LEAP Proxy RADIUS Server database, the mapping is only applied as a default if those databases did not specify a Cisco Secure ACS group for the user.



Downloaded from www.Manualslib.com manuals search engine

**Note** For more information about group specification for RADIUS token servers, see RADIUS-Based Group Specification, page 16-14. For more information about group specification for ODBC databases, see Cisco Secure ACS Authentication Process with an ODBC External User Database, page 13-58.

# Group Mapping by Group Set Membership

You can create group mappings for some external user databases based on the combination of external user database groups to which users belong. The following are the external user database types for which you can create group mappings based on group set membership:

- Windows domains

  **Note** Group mapping for Windows authentication supports only those users who belong to no more than 500 Windows groups.

- Novell NDS
- Generic LDAP

When you configure a Cisco Secure ACS group mapping based on group set membership, you can add one or many external user database groups to the set. For Cisco Secure ACS to map a user to the specified Cisco Secure ACS group, the user must match *all* external user database groups in the set.

As an example, you could configure a group mapping for users who belong to both the Engineering and Tokyo groups and a separate one for users who belong to both Engineering and London. You could then configure separate group mappings for the combinations of Engineering-Tokyo and Engineering-London and configure different access times for the Cisco Secure ACS groups to which they map. You could also configure a group mapping that only included the Engineering group that would map other members of the Engineering group who were not members of Tokyo or London.



Downloaded from www.Manualslib.com manuals search engine

# Group Mapping Order

Cisco Secure ACS always maps users to a single Cisco Secure ACS group, yet a user can belong to more than one group set mapping. For example, a user, John, could be a member of the group combination Engineering and California, and at the same time be a member of the group combination Engineering and Managers. If there are Cisco Secure ACS group set mappings for both these combinations, Cisco Secure ACS has to determine to which group John should be assigned.

Cisco Secure ACS prevents conflicting group set mappings by assigning a mapping order to the group set mappings. When a user authenticated by an external user database is to be assigned to a Cisco Secure ACS group, Cisco Secure ACS starts at the top of the list of group mappings for that database. Cisco Secure ACS checks the user group memberships in the external user database against each group mapping in the list sequentially. Upon finding the first group set mapping that matches the external user database group memberships of the user, Cisco Secure ACS assigns the user to the Cisco Secure ACS group of that group mapping and terminates the mapping process.

Clearly, the order of group mappings is important because it affects the network access and services allowed to users. When defining mappings for users who belong to multiple groups, make sure they are in the correct order so that users are granted the correct group settings.

For example, a user, Mary, is assigned to the three-group combination of Engineering, Marketing, and Managers. Mary should be granted the privileges of a manager rather than an engineer. Mapping A assigns users who belong to all three groups Mary is in to Cisco Secure ACS Group 2. Mapping B assigns users who belong to the Engineering and Marketing groups to Cisco Secure ACS Group 1. If Mapping B is listed first, Cisco Secure ACS authenticates Mary as a user of Group 1, and she is be assigned to Group 1, rather than Group 2 like managers should be.

# No Access Group for Group Set Mappings

To prevent remote access for users assigned a group by a particular group set mapping, assign the group to the Cisco Secure ACS No Access group. For example, you could assign all members of an external user database group “Contractors” to the No Access group so they could not dial in to the network remotely.



Downloaded from www.Manualslib.com manuals search engine

# Default Group Mapping for Windows

For Windows user databases, Cisco Secure ACS includes the ability to define a default group mapping. If no other group mapping matches an unknown user authenticated by a Windows user database, Cisco Secure ACS assigns the user to a group based on the default group mapping.

Configuring the default group mapping for Windows user databases is the same as editing an existing group mapping, with one exception. When editing the default group mapping for Windows, instead of selecting a valid domain name on the Domain Configurations page, select \DEFAULT.

For more information about editing an existing group mapping, see Editing a Windows, Novell NDS, or Generic LDAP Group Set Mapping, page 16-9.

# Windows Group Mapping Limitations

Cisco Secure ACS has the following limits with respect to group mapping for users authenticated by a Windows user database:

- Cisco Secure ACS can only support group mapping for users who belong to 500 or less Windows groups.
- Cisco Secure ACS can only perform group mapping using the local and global groups a user belongs to in the domain that authenticated the user. Group membership in domains trusted by the authenticating domain cannot be used for Cisco Secure ACS group mapping. This restriction is not removed by adding a remote group to a group local to the domain providing authentication.



Downloaded from www.Manualslib.com manuals search engine

# Creating a Cisco Secure ACS Group Mapping for Windows, Novell NDS, or Generic LDAP Groups

**Before You Begin**

To map a Windows, Novell NDS, or generic LDAP group to a Cisco Secure ACS group, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Group Mappings**.

**Step 3** Click the external user database name for which you want to configure a group mapping.

If you are mapping a Windows group set, the Domain Configurations table appears. If you are mapping an NDS group set, the NDS Trees table appears. Otherwise, the Group Mappings for *database* Users table appears.

**Step 4** If you are mapping a Windows group set for a new domain, follow these steps:

**a.** Click **New configuration**.

The Define New Domain Configuration page appears.

**b.** If the Windows domain for which you want to create a group set mapping configuration appears in the Detected domains list, select the name of the domain.

**Tip** To clear your domain selection, click Clear Selection.

**c.** If the Windows domain for which you want to create a group set mapping *does not appear* in the Detected domains list, type the name of a trusted Windows domain in the Domain box.

**d.** Click **Submit**.

The new Windows domain appears in the list of domains in the Domain Configurations page.

**Step 5** If you are mapping a Windows group set, click the domain name for which you want to configure a group set mapping.

The Group Mappings for Domain: *domainname* table appears.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** If you are mapping a Novell NDS group set, click the name of the Novell NDS tree for which you want to configure group set mappings.

The Group Mappings for NDS Users table appears.

**Step 7** Click **Add Mapping**.

The Create new group mapping for *database* page opens. The group list displays group names derived from the external user database.

**Step 8** For each group to be added to the group set mapping, select the name of the applicable external user database group in the group list, and then click **Add to selected**.

**Note** A user must match *all* the groups in the Selected list so that Cisco Secure ACS can use this group set mapping to map the user to a Cisco Secure ACS group; however, a user can also belong to other groups (in addition to the groups listed) and still be mapped to a Cisco Secure ACS group.

**Tip** To remove a group from the mapping, select the name of the group in the Selected list, and then click **Remove from selected**.

The Selected list shows all the groups that a user must belong to in order to be mapped to a Cisco Secure ACS group.

**Step 9** In the CiscoSecure group list, select the name of the Cisco Secure ACS group to which you want to map users who belong to all the external user database groups in the Selected list.

**Note** You can also select <No Access>. For more information about the <No Access> group, see No Access Group for Group Set Mappings, page 16-5.

**Step 10** Click **Submit**.

The group set you mapped to the Cisco Secure ACS list appears at the bottom of the *database* groups column.



Downloaded from www.Manualslib.com manuals search engine

**Note** The asterisk at the end of each set of groups indicates that users authenticated with the external user database can belong to other groups besides those in the set.

# Editing a Windows, Novell NDS, or Generic LDAP Group Set Mapping

You can change the Cisco Secure ACS group to which a group set mapping is mapped.

**Note** The external user database groups of an existing group set mapping cannot be edited. If you want to add or remove external user database groups from the group set mapping, delete the group set mapping and create one with the revised set of groups.

To edit a Windows, Novell NDS, or generic LDAP group mapping, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Group Mappings**.

**Step 3** Click the external user database name for which you want to edit a group set mapping.

If you are editing a Windows group set mapping, the Domain Configurations table appears. If you are editing an NDS group set mapping, the NDS Trees table appears. Otherwise, the Group Mappings for *database* Users table appears.

**Step 4** If you are editing a Windows group set mapping, click the domain name for which you want to edit a group set mapping.

The Group Mappings for Domain: *domainname* table appears.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** If you are editing a Novell NDS group set mapping, click the name of the Novell NDS tree for which you want to edit a group set mapping.

The Group Mappings for NDS Users table appears.

**Step 6** Click the group set mapping to be edited.

The Edit mapping for *database* page opens. The external user database group or groups included in the group set mapping appear above the CiscoSecure group list.

**Step 7** From the CiscoSecure group list, select the name of the group to which the set of external database groups should be mapped, and then click **Submit**.

**Note** You can also select <No Access>. For more information about the <No Access> group, see No Access Group for Group Set Mappings, page 16-5.

**Step 8** Click **Submit**.

The Group Mappings for *database* page opens again with the changed group set mapping listed.

# Deleting a Windows, Novell NDS, or Generic LDAP Group Set Mapping

You can delete individual group set mappings.

To delete a Windows, Novell NDS, or generic LDAP group mapping, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Group Mappings**.

**Step 3** Click the external user database configuration whose group set mapping you need to delete.



Downloaded from www.Manualslib.com manuals search engine

If you are deleting a Windows group set mapping, the Domain Configurations table appears. If you are deleting an NDS group set mapping, the NDS Trees table appears. Otherwise, the Group Mappings for *database* Users table appears.

**Step 4** If you are deleting a Windows group set mapping, click the domain name whose group set mapping you want to delete.

The Group Mappings for Domain: *domainname* table appears.

**Step 5** If you are deleting a Novell NDS group set mapping, click the name of the Novell NDS tree whose group set mapping you want to delete.

The Group Mappings for NDS Users table appears.

**Step 6** Click the group set mapping you want to delete.

**Step 7** Click **Delete**.

Cisco Secure ACS displays a confirmation dialog box.

**Step 8** Click **OK** in the confirmation dialog box.

Cisco Secure ACS deletes the selected external user database group set mapping.

# Deleting a Windows Domain Group Mapping Configuration

You can delete an entire group mapping configuration for a Windows domain. When you delete a Windows domain group mapping configuration, all group set mappings in the configuration are deleted.

To delete a Windows group mapping, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Group Mappings**.

**Step 3** Click the name of the Windows external user database.

**Step 4** Click the domain name whose group set mapping you want to delete.

**Step 5** Click **Delete Configuration**.

Cisco Secure ACS displays a confirmation dialog box.



Downloaded from www.Manualslib.com manuals search engine

**Step 6** Click **OK** in the confirmation dialog box.

Cisco Secure ACS deletes the selected external user database group mapping configuration.

# Changing Group Set Mapping Order

You can change the order in which Cisco Secure ACS checks group set mappings for users authenticated by Windows, Novell NDS, and generic LDAP databases. To order group mappings, you must have already mapped them. For more information about creating group mappings, see Creating a Cisco Secure ACS Group Mapping for Windows, Novell NDS, or Generic LDAP Groups, page 16-7.

To change the order of group mappings for a Windows, Novell NDS, or generic LDAP group mapping, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Group Mappings**.

**Step 3** Click the external user database name for which you want to configure group set mapping order.

If you are ordering Windows group set mappings, the Domain Configurations table appears. If you are ordering NDS group set mappings, the NDS Trees table appears. Otherwise, the Group Mappings for *database* Users table appears.

**Step 4** If you are configuring Windows group mapping order, click the domain name for which you want to configure group set mapping order.

The Group Mappings for Domain: *domainname* table appears.

**Step 5** If you are configuring Novell NDS group set mapping order, click the name of the Novell NDS tree for which you want to configure group set mapping order.

The Group Mappings for NDS Users table appears.

**Step 6** Click **Order mappings**.

**Note** The Order mappings button appears only if more than one group set mapping exists for the current database.



Downloaded from www.Manualslib.com manuals search engine

The Order mappings for *database* page appears. The group mappings for the current database appear in the Order list.

**Step 7** Select the name of a group set mapping you want to move, and then click **Up** or **Down** until it is in the position you want.

**Step 8** Repeat Step 7 until the group mappings are in the order you need.

**Step 9** Click **Submit**.

The Group Mappings for *database* page displays the group set mappings in the order you defined.

# NAC Group Mapping

Group mapping for Network Admission Control (NAC) databases provides the means to connect a system posture token (SPT) that is the result of posture validation to the user group whose authorizations you have configured to correspond to that SPT. Through the use of group mapping, the applicable downloadable IP ACLs and Cisco RADIUS cisco-av-pair attribute values are assigned to network sessions of a Network Admission Control (NAC)-client workstation. Each NAC database instance that you create has unique SPT-to-group mappings for each of the five SPTs.

For more information about posture tokens, see Posture Tokens, page 14-4.

## Configuring NAC Group Mapping

To configure NAC group mapping, follow these steps:

**Step 1** In the navigation bar, click **External User Databases**.

**Step 2** Click **Database Group Mappings**.

Cisco Secure ACS displays a list of all external databases, including NAC databases.

**Step 3** Click the name of the NAC database whose SPT-to-group mappings you want to configure.



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS displays the Token-to-User-Group Mapping page for the NAC database you selected.

**Step 4** For each SPT, follow these steps:

**a.** From the **User Group** list, select a group or, if you want to deny access, select the <No Access> option, which is the default selection.

When the result of posture validation is the SPT listed to the left of the User Group list, Cisco Secure ACS sends to the AAA client the authorizations associated with the selected group.

**b.** (Optional) In the PA User Message box, type a message that the NAC client can show the user of the computer running the NAC client.

**Note** Whether the NAC client displays messages depends upon the configuration and design of the NAC client.

**Step 5** Click **Submit**.

Cisco Secure ACS saves the SPT-to-user-group mapping.

# RADIUS-Based Group Specification

For some types of external user databases, Cisco Secure ACS supports the assignment of users to specific Cisco Secure ACS groups based upon the RADIUS authentication response from the external user database. This is provided in addition to the unknown user group mapping described in Group Mapping by External User Database, page 16-2. RADIUS-based group specification overrides group mapping. The database types that support RADIUS-based group specification are as follows:

- LEAP Proxy RADIUS server
- RADIUS token server

Cisco Secure ACS supports per-user group mapping for users authenticated with a LEAP Proxy RADIUS Server database. This is provided in addition to the default group mapping described in Group Mapping by External User Database, page 16-2.



Downloaded from www.Manualslib.com manuals search engine

To enable per-user group mapping, configure the external user database to return authentication responses that contain the Cisco IOS/PIX RADIUS attribute 1, [009\001] cisco-av-pair with the following value:

```
ACS:CiscoSecure-Group-Id =  N
```

where *N* is the Cisco Secure ACS group number (0 through 499) to which Cisco Secure ACS should assign the user. For example, if the LEAP Proxy RADIUS Server authenticated a user and included the following value for the Cisco IOS/PIX RADIUS attribute 1, [009\001] cisco-av-pair:

```
ACS:CiscoSecure-Group-Id = 37
```

Cisco Secure ACS assigns the user to group 37 and applies authorization associated with group 37.



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

# Troubleshooting

This appendix provides information about certain basic problems and describes how to resolve them.

Scan the column on the left to identify the condition that you are trying to resolve, and then carefully go through each corresponding recovery action offered in the column on the right.

This chapter contains the following topics:


- Administration Issues, page A-2
- Browser Issues, page A-4
- Cisco IOS Issues, page A-5
- Database Issues, page A-7
- Dial-in Connection Issues, page A-10
- Debug Issues, page A-14
- Proxy Issues, page A-15
- Installation and Upgrade Issues, page A-16
- MaxSessions Issues, page A-16
- Report Issues, page A-17
- Third-Party Server Issues, page A-19
- User Authentication Issues, page A-20
- TACACS+ and RADIUS Attribute Issues, page A-22




Downloaded from www.Manualslib.com manuals search engine

# Administration Issues

| Condition | Recovery Action |
|---|---|
| Remote administrator cannot bring up the Cisco Secure ACS HTML interface in a browser or receives a warning that access is not permitted. | • Verify that you are using a supported browser. Refer to the *Release Notes for Cisco Secure Access Control Server for Windows Server Version 3.3* for a list of supported browsers.<br>• Ping Cisco Secure ACS to confirm connectivity.<br>• Verify that the remote administrator is using a valid administrator name and password that have previously been added in Administration Control.<br>• Verify that Java functionality is enabled in the browser.<br>• Determine whether the remote administrator is trying to administer Cisco Secure ACS through a firewall, through a device performing Network Address Translation, or from a browser configured to use an HTTP proxy server. For more information about accessing the HTML interface in these networking scenarios, see Network Environments and Administrative Sessions, page 1-30. |
| No remote administrators can log in. | The option **Allow only listed IP addresses to connect** is selected, but no start or stop IP addresses are listed. Go to **Administrator Control > Access Policy** and specify the **Start IP Address** and **End IP Address**. |
| Unauthorized users can log in. | The option **Reject listed IP addresses** is selected, but no start or stop IP addresses are listed. Go to **Administrator Control > Access Policy** and specify the **Start IP Address** and **Stop IP Address**. |
| The Restart Services function does not work. | This may occur if the system is not responding. To manually restart services, from the Windows **Start** menu, choose **Settings > Control Panel > Administrative Tools > Services**. Click **CSAdmin**, and then **Stop**, and then **Start**.<br>If the services do not respond when manually restarted, reboot the server. |



Downloaded from www.Manualslib.com manuals search engine

| Condition | Recovery Action |
|---|---|
| Administrator configured for event notification is not receiving e-mail. | Ensure that the SMTP server name is correct. If the name is correct, ensure that the computer running Cisco Secure ACS can ping the SMTP server or can send e-mail via a third-party e-mail software package. Make sure you have not used underscores in the e-mail address. |
| Remote Administrator receives "Logon failed . . . protocol error" message, when browsing. | Restart the CSADMIN service. To restart the CSADMIN service, from the Windows **Start** menu choose **Control Panel > Services**. Click **CSAdmin**, and then **Stop**, and then **Start**.<br><br>If necessary, restart the server. |
| Remote administrator cannot bring up Cisco Secure ACS from his or her browser, or receives a warning that access is not permitted. | If Network Address Translation is enabled on the PIX Firewall, administration through the firewall cannot work.<br><br>To administer Cisco Secure ACS through a firewall, you must configure an HTTP port range in **Administrator Control > Access Policy**. The PIX Firewall must be configured to permit HTTP traffic over all ports included in the range specified in Cisco Secure ACS. For more information, see Access Policy, page 12-11. |
| Unable to log in on Cisco Secure ACS. Authentication fails. | Back up the NT Registry.<br><br>Use the regedit command and remove the users in the following:<br><br>`HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAA##\CSAdmin\Administrators`<br><br>Under the **Administrators** key you will see all administrators that you have created. Delete the users and exit the Registry. Upon accessing Cisco Secure ACS, you will not be prompted for a username and password. After you have brought up the Cisco Secure ACS HTML interface, you can re-add administrators. |



Downloaded from www.Manualslib.com manuals search engine

# Browser Issues

| Condition | Recovery Action |
|---|---|
| The browser cannot bring up the Cisco Secure ACS HTML interface. | Open Internet Explorer or Netscape Navigator and choose **Help > About** to determine the version of the browser. See System Requirements, page 2-2, for a list of browsers supported by Cisco Secure ACS and the release notes for known issues with a particular browser version.<br><br>For information about various network scenarios that affect remote administrative sessions, see Network Environments and Administrative Sessions, page 1-30. |
| The browser displays the Java message that your session connection is lost. | Check the **Session idle timeout** value for remote administrators. This is on the **Session Policy Setup** page of the **Administration Control** section. Increase the value as needed. |
| Administrator database appears corrupted. | The remote Netscape client is caching the password. If you specify an incorrect password, it is cached. When you attempt to re-authenticate with the correct password, the incorrect password is sent. Clear the cache before attempting to re-authenticate or close the browser and open a new session. |
| Remote administrator intermittently can't browse the Cisco Secure ACS HTML interface. | Make sure that the client browser does not have proxy server configured. Cisco Secure ACS does not support HTTP proxy for remote administrative sessions. Disable proxy server settings. |



Downloaded from www.Manualslib.com manuals search engine

# Cisco IOS Issues

| Condition | Recovery Action |
|---|---|
| The results of `show eou all` or `show eou ip` *address* include postures that do not match the actual result of posture validation or display "-------" instead of a posture. | If the posture displayed is "-------", the AAA client is not receiving the posture-token attribute-value (AV) pair within a Cisco IOS/PIX RADIUS cisco-av-pair vendor-specific attribute (VSA). If the posture displayed does not correspond to the actual result of posture validation, the AAA client is receiving an incorrect value in the posture-token AV pair.<br><br>Check group mappings for Network Admission Control (NAC) databases to verify that the correct user groups are associated with each system posture token (SPT). In the user groups configured for use with NAC, be sure that the Cisco IOS/PIX cisco-av-pair VSA is configured correctly. For example, in a group configured to authorize NAC clients receiving a Healthy SPT, be sure the **[009\001] cisco-av-pair** check box is selected and that the following string appears in the **[009\001] cisco-av-pair** text box:<br><br>`posture-token=Healthy`<br><br>⚠ **Caution** The posture-token AV pair is the only way that Cisco Secure ACS notifies the AAA client of the SPT returned by posture validation. Because you manually configure the posture-token AV pair, errors in configuring posture-token can result in the incorrect SPT being sent to the AAA client or, if the AV pair name is mistyped, the AAA client not receiving the SPT at all.<br><br>**Note** AV pair names are case sensitive.<br><br>For information about group mapping for NAC databases, see NAC Group Mapping, page 16-13. For more information about the Cisco IOS/PIX cisco-av-pair VSA, see About the cisco-av-pair RADUIS Attribute, page C-7. |



Downloaded from www.Manualslib.com manuals search engine

| Condition | Recovery Action |
|---|---|
| Under EXEC Commands, Cisco IOS commands are not being denied when checked. | Examine the Cisco IOS configuration at the AAA client. If it is not already present, add the following Cisco IOS command to the AAA client configuration:<br>**`aaa authorization command <0-15> default group TACACS+`**<br>The correct syntax for the arguments in the text box is **permit** *argument* or **deny** *argument*. |
| Administrator has been locked out of the AAA client because of an incorrect configuration set up in the AAA client. | If you have a fallback method configured on your AAA client, disable connectivity to the AAA server and log in using local/line username and password.<br>Try to connect directly to the AAA client at the console port. If that is not successful, consult your AAA client documentation or see the Password Recovery Procedures page on Cisco.com for information regarding your particular AAA client. |
| IETF RADIUS attributes not supported in Cisco IOS 12.0.5.T | Cisco incorporated RADIUS (IETF) attributes in Cisco IOS Release 11.1. However, there are a few attributes that are not yet supported or that require a later version of the Cisco IOS software. For more information, see the RADIUS Attributes page on Cisco.com. |
| Unable to enter Enable Mode after doing `aaa authentication enable default tacacs+`. Getting error message "Error in authentication on the router." | Check the failed attempts log in the ACS. If the log reads "CS password invalid," it may be that the user has no enable password set up. Set the TACACS+ Enable Password within the **Advanced TACACS+ Settings** section.<br>If you do not see the Advanced TACACS+ Settings section among the user setup options, go to **Interface Configuration > Advanced Configuration Options > Advanced TACACS+ Features** and select that option to have the TACACS+ settings appear in the user settings. Then select Max privilege for any AAA Client (this will typically be 15) and enter the TACACS+ Enable Password that you want the user to have for enable. |



Downloaded from www.Manualslib.com manuals search engine

# Database Issues

| Condition | Recovery Action |
|---|---|
| RDBMS Synchronization is not operating properly. | Make sure that the correct server is listed in the **Partners** list. |
| Database Replication not operating properly. | • Make sure you have set the server correctly as either Send or Receive.<br>• On the sending server, make sure the receiving server is in the Replication list.<br>• On the receiving server, make sure the sending server is selected in the Accept Replication from list. Also, make sure that the sending server is not in the replication partner list.<br>• Make sure that the replication schedule on the sending Cisco Secure ACS is not conflicting with the replication schedule on the receiving Cisco Secure ACS.<br>• If the receiving server has dual network cards, on the sending server add a AAA server to the AAA Servers table in the Network Configuration section for every IP address of the receiving server. If the sending server has dual network cards, on the receiving server add a AAA server to the AAA Servers table in Network Configuration for every IP address of the receiving server. |
| The external user database is not available in the Group Mapping section. | The external database has not been configured in the External User Databases section, or the username and password have been typed incorrectly. Click the applicable external database to configure. Make sure that the username and password are correct. |



Downloaded from www.Manualslib.com manuals search engine

| Condition | Recovery Action |
|---|---|
| External databases not operating properly. | Make sure that a two-way trust (for dial-in check) has been established between the Cisco Secure ACS domain and the other domains.<br><br>If Cisco Secure ACS is installed on a Member Server and is authenticating to a Domain Controller, see the "Authentication Failures When ACS/NT 3.0 Is Authenticating to Active Directory" Field Notice at the following URL:<br><br>http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_field_notice09186a00800b1583.shtml |
| Cannot install Novell NDS database authentication. | Make sure Novell Requestor is installed on the same Windows server as the Cisco Secure ACS. |
| Unknown users are not authenticated. | Go to **External User Databases > Unknown User Policy**. Select the **Check the following external user databases** option. From the External Databases list, select the database(s) against which to authenticate unknown users. Click —> (right arrow button) to add the database to the Selected Databases list. Click **Up** or **Down** to move the selected database into the desired position in the authentication hierarchy.<br><br>If you are using the Cisco Secure ACS Unknown User feature, external databases can only authenticate using PAP. |
| Novell NDS or Generic LDAP Group Mapping not working correctly. | Make sure that you have correctly configured Group Mapping for the applicable database.<br><br>For more information, see Chapter 16, "User Group Mapping and Specification". |



Downloaded from www.Manualslib.com manuals search engine

| Condition | Recovery Action |
|---|---|
| Unable to authenticate against the Novell NDS database. | Make sure that the tree name, context name, and container name are all specified correctly. Start with one container where users are present; then you can add more containers later, if needed.<br><br>If you are successful, check on the AAA client to see if you can authenticate the shell user (Telnet user). Also make sure that for PPP you have PAP authentication configured on the asynchronous interface. |
| Same user appears in multiple groups or duplicate users exist in the Cisco Secure ACS database. Unable to delete user from database. | Clean up the database typing the following command from the command line:<br><br>**csutil -q -d -n -l dump.txt**<br><br>This command causes the database to be unloaded and reloaded to clear up the counters.<br><br>**Tip** When you install Cisco Secure ACS in the default location, **CSUtil.exe** is located in the following directory: `C:\Program Files\CiscoSecure ACS vX.X\Utils`.<br><br>For more information on using the **csutil** command see Appendix D, "CSUtil Database Utility". |



Downloaded from www.Manualslib.com manuals search engine

# Dial-in Connection Issues

| Condition | Recovery Action |
|---|---|
| A dial-in user cannot connect to the AAA client.<br><br>No record of the attempt appears in either the TACACS+ or RADIUS Accounting Report (in the Reports & Activity section, click **TACACS+ Accounting** or **RADIUS Accounting** or **Failed Attempts**). | Examine the Cisco Secure ACS Reports or AAA client Debug output to narrow the problem to a system error or a user error. Confirm the following:<br>• The dial-in user was able to establish a connection and ping the computer *before Cisco* Secure ACS was installed. If the dial-in user could not, the problem is related to a AAA client/modem configuration, not Cisco Secure ACS.<br>• LAN connections for both the AAA client and the computer running Cisco Secure ACS are physically connected.<br>• IP address of the AAA client in the Cisco Secure ACS configuration is correct.<br>• IP address of Cisco Secure ACS in AAA client configuration is correct.<br>• TACACS+ or RADIUS key in both AAA client and Cisco Secure ACS are identical (case sensitive).<br>• The command **ppp authentication pap** is entered for each interface, if you are using a Windows user database.<br>• The command **ppp authentication chap pap** is entered for each interface, if you are using the Cisco Secure ACS database.<br>• The AAA and TACACS+ or RADIUS commands are correct in the AAA client. The necessary commands are listed in the following:<br>`Program Files\CiscoSecure ACS vx.x\TacConfig.txt`<br>`Program Files\CiscoSecure ACS vx.x\RadConfig.txt`<br>• The Cisco Secure ACS Services are running (CSAdmin, CSAuth, CSDBSync CSLog, CSRadius, CSTacacs) on the computer running Cisco Secure ACS. |



Downloaded from www.Manualslib.com manuals search engine

| Condition | Recovery Action |
|---|---|
| A dial-in user cannot connect to the AAA client.<br><br>The Windows user database is being used for authentication.<br><br>A record of a failed attempt appears in the Failed Attempts Report (in the Reports & Activity section, click **Failed Attempts**). | Create a local user in the CiscoSecure user database and test whether authentication is successful. If it is successful, the issue is that the user information is not correctly configured for authentication in Windows or Cisco Secure ACS.<br><br>From the Windows User Manager or Active Directory Users and Computers, confirm the following:<br><br>• The username and password are configured in the Windows User Manager or Active Directory Users and Computers.<br>• The user can log in to the domain by authenticating through a workstation.<br>• The User Properties window does not have User Must Change Password at Login enabled.<br>• The User Properties window does not have Account Disabled selected.<br>• The User Properties for the dial-in window does not have Grant dial-in permission to user disabled, if Cisco Secure ACS is using this option for authenticating.<br><br>From within Cisco Secure ACS confirm the following:<br><br>• If the username has already been entered into Cisco Secure ACS, a Windows user database configuration is selected in the Password Authentication list on the User Setup page for the user.<br>• If the username has already been entered into Cisco Secure ACS, the Cisco Secure ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Be sure to click **Submit + Restart** if a change has been made.<br>• The user expiration information in the Windows user database has not caused failed authentication. For troubleshooting purposes, disable password expiry for the user in the Windows user database.<br><br>Click **External User Databases**, and click **List All Databases Configured**, and then make sure that the database configuration for Windows is listed.<br><br>In the Configure Unknown User Policy table of the External User Databases section ensure that Fail the attempt is not selected. And ensure that the Selected Databases list reflects the necessary database.<br><br>Verify that the Windows group that the user belongs to has not been mapped to No Access. |



Downloaded from www.Manualslib.com manuals search engine

| Condition | Recovery Action |
|---|---|
| A dial-in user cannot connect to the AAA client.<br><br>The CiscoSecure user database is being used for authentication.<br><br>A record of a failed attempt is displayed in the Failed Attempts Report (in the Reports & Activity section, click **Failed Attempts**). | From within Cisco Secure ACS confirm the following:<br>• The username has been entered into Cisco Secure ACS.<br>• CiscoSecure user database is selected from the Password Authentication list and a password has been entered in User Setup for the user.<br>• The Cisco Secure ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Be sure to click **Submit + Restart** if a change has been made.<br>• Expiration information has not caused failed authentication. Set to Expiration: Never for troubleshooting. |
| A dial-in user cannot connect to the AAA client; however, a Telnet connection can be authenticated across the LAN. | The problem is isolated to one of three areas:<br>• Line/modem configuration problem. Review the documentation that came with your modem and verify that the modem is properly configured.<br>• The user is not assigned to a group that has the correct authorization rights. Authorization rights can be modified under Group Setup or User Setup. User settings override group settings.<br>• The Cisco Secure ACS or TACACS+ or RADIUS configuration is not correct in the AAA client.<br><br>Additionally, you can verify Cisco Secure ACS connectivity by attempting to Telnet to the access server from a workstation connected to the LAN. A successful authentication for Telnet confirms that Cisco Secure ACS is working with the AAA client. |



Downloaded from www.Manualslib.com manuals search engine

| Condition | Recovery Action |
|---|---|
| A dial-in user cannot connect to the AAA client, and a Telnet connection cannot be authenticated across the LAN. | Determine whether the Cisco Secure ACS is receiving the request. This can be done by viewing the Cisco Secure ACS reports. Based on what does not appear in the reports and which database is being used, troubleshoot the problem based on one of the following:<br>• Line/modem configuration problem. Review the documentation that came with your modem and verify that the modem is properly configured.<br>• The user does not exist in the Windows user database or the CiscoSecure user database and might not have the correct password. Authentication parameters can be modified under User Setup.<br>• The Cisco Secure ACS or TACACS+ or RADIUS configuration is not correct in the AAA client. |
| Callback is not working. | Ensure that callback works on the AAA client when using local authentication. Then add AAA authentication. |
| User authentication fails when using PAP. | Outbound PAP is not enabled. If the Failed Attempts report shows that you are using outbound PAP, go to the Interface Configuration section and select the **Per-User Advanced TACACS+ Features** check box. Then, go to the TACACS+ Outbound Password section of the Advanced TACACS+ Settings table on the User Setup page and type and confirm the password in the boxes provided. |



Downloaded from www.Manualslib.com manuals search engine

# Debug Issues

| Condition | Recovery Action |
|---|---|
| When you run **debug aaa authentication** on the AAA client, Cisco Secure ACS returns a failure message. | The configurations of the AAA client or Cisco Secure ACS are likely to be at fault.<br>From within Cisco Secure ACS confirm the following:<br>Cisco Secure ACS is receiving the request. This can be done by viewing the Cisco Secure ACS reports. What does or does not appear in the reports may provide indications that your Cisco Secure ACS is misconfigured.<br>From the AAA client, confirm the following:<br>• The command **ppp authentication pap** is entered for each interface if authentication against the Windows user database is being used.<br>• The command **ppp authentication chap pap** is entered for each interface if authentication against the CiscoSecure user database is being used.<br>• The AAA and TACACS+ or RADIUS configuration is correct in the AAA client. |
| When you run **debug aaa authentication** and **debug aaa authorization** on the AAA client, Cisco Secure ACS returns a `PASS` for authentication, but returns a `FAIL` for authorization. | This problem occurs because authorization rights are not correctly assigned.<br>Examine the following:<br>• Check failed attempts reports under Reports and Activities to see if any services/protocols are being denied for the user.<br>• From User Setup, confirm that the user is assigned to a group that has the correct authorization rights. Authorization rights can be modified under Group Setup or User Setup. User settings override group settings.<br>• If a specific attribute for TACACS+ or RADIUS is not displayed within the Group Setup section, this may indicate that it has not been enabled in Interface Configuration: TACACS+ (Cisco IOS) or RADIUS. |



Downloaded from www.Manualslib.com manuals search engine

# Proxy Issues

| Condition | Recovery Action |
|---|---|
| Proxying requests to another server fail | Make sure that the following conditions are met:<br>• The direction on the remote server is set to Incoming/Outgoing or Incoming, and that the direction on the authentication forwarding server is set to Incoming/Outgoing or Outgoing.<br>• The shared secret (key) matches the shared secret of one or both Cisco Secure ACSes.<br>• The character string and delimiter match the stripping information configured in the Proxy Distribution Table, and the position is set correctly to either Prefix or Suffix.<br>If the conditions above are met, one or more servers is probably down, or no fallback server is configured. Go to the Network Configuration section and configure a fallback server. Fallback servers are used only under the following circumstances:<br>• The remote Cisco Secure ACS is down.<br>• One or more services (CSTacacs, CSRadius, or CSAuth) are down.<br>• The secret key is misconfigured.<br>• Inbound/Outbound messaging is misconfigured. |



Downloaded from www.Manualslib.com manuals search engine

# Installation and Upgrade Issues

| Condition | Recovery Action |
|---|---|
| The following error message appears when you try to upgrade or uninstall Cisco Secure ACS:<br>`The following file is invalid or the data is corrupted`<br>`"DelsL1.isu"` | From the Windows Registry, delete the following Registry key:<br>`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Uninstall\CiscoSecure` |
| All previous accounting logs are missing. | When reinstalling or upgrading the Cisco Secure ACS software, these files are deleted unless they have been moved to an alternative directory location. |

# MaxSessions Issues

| Condition | Recovery Action |
|---|---|
| MaxSessions over VPDN is not working. | The use of MaxSessions over VPDN is not supported. |
| User MaxSessions fluctuates or is unreliable. | Services were restarted, possibly because the connection between the Cisco Secure ACS and the AAA client is unstable. Click to clear the **Single Connect TACACS+ AAA Client** check box. |
| User MaxSessions not taking affect. | Make sure you have accounting configured on the AAA client and you are receiving accounting start/stop records. |



Downloaded from www.Manualslib.com manuals search engine

# Report Issues

| Condition | Recovery Action |
|---|---|
| The *logname*`active.csv` report is blank. | You changed protocol configurations recently.<br>Whenever protocol configurations change, the existing *logname*`active.csv` report file is renamed to *logname*`yyyy-mm-dd.csv`, and a new, blank *logname*`active.csv` report is generated |
| A report is blank. | Make sure you have selected Log to *reportname* Report under System Configuration: Logging: Log Target: *reportname*. You must also set Network Configuration: *servername*: Access Server Type to Cisco Secure ACS for Windows NT. |
| No Unknown User information is included in reports. | The Unknown User database was changed. Accounting reports will still contain unknown user information. |
| Two entries are logged for one user session. | Make sure that the remote logging function is not configured to send accounting packets to the same location as the Send Accounting Information fields in the Proxy Distribution Table. |
| After you have changed the date format, the Logged-In User list and the `CSAdmin` log still display old format dates. | To see the changes made, you must restart the csadmin services and log on again. |



Downloaded from www.Manualslib.com manuals search engine

| Condition | Recovery Action |
|---|---|
| The `Logged in Users` report works with some devices, but not with others | For the `Logged in Users` report to work (and this also applies to most other features involving sessions), packets should include at least the following fields:<br>• **Authentication Request packet**<br>– nas-ip-address<br>– nas-port<br>• **Accounting Start packet**<br>– nas-ip-address<br>– nas-port<br>– session-id<br>– framed-ip-address<br>• **Accounting Stop packet**<br>– nas-ip-address<br>– nas-port<br>– session-id<br>– framed-ip-address<br>Also, if a connection is so brief that there is little time between the start and stop packets (for example, HTTP through the PIX Firewall), the `Logged in Users` report may fail. |



Downloaded from www.Manualslib.com manuals search engine

# Third-Party Server Issues

| Condition | Recovery Action |
|---|---|
| You cannot successfully implement the RSA token server. | 1. Log in to the computer running Cisco Secure ACS. (Make sure your login account has administrative privileges.)<br>2. Make sure the RSA Client software is installed on the same computer as Cisco Secure ACS.<br>3. Follow the setup instructions. Do not restart at the end of the installation.<br>4. Get the file named `sdconf.rec` located in the `/data` directory of the RSA ACE server.<br>5. Place `sdconf.rec` in the `%SystemRoot%\system32` directory.<br>6. Make you can ping the machine that is running the ACE server by hostname. (You might need to add the machine in the lmhosts file.)<br>7. Verify that support for RSA is enabled in External User Database: Database Configuration in the Cisco Secure ACS.<br>8. Run Test Authentication from the Windows control panel for the ACE/Client application.<br>9. From Cisco Secure ACS, install the token server. |
| Authentication request does not hit the external database. | Set logging to full in System Configuration > Service Control<br>Check csauth.log for confirmation that the authentication request is being forwarded to the third-party server. If it is not being forwarded, confirm that the external database configuration is correct, as well as the unknown user policy settings. |
| On ACE/SDI server no incoming request is seen from Cisco Secure ACS, although RSA/agent authentication works. | For dial-up users, make sure you are using PAP and not MS-CHAP or CHAP; RSA/SDI does not support CHAP, and Cisco Secure ACS will not send the request to the RSA server, but rather it will log an error with external database failure. |



Downloaded from www.Manualslib.com manuals search engine

# User Authentication Issues

| Condition | Recovery Action |
|---|---|
| After the administrator disables the Dialin Permission setting, Windows database users can still dial in and apply the Callback string configured under the Windows user database. (You can locate the Dialin Permission check box by clicking External User Databases, clicking Database Configuration, clicking Windows Database, and clicking Configure.) | Restart Cisco Secure ACS services. For steps, see Stopping, Starting, or Restarting Services, page 8-2. |
| User did not inherit settings from new group. | Users moved to a new group inherit new group settings but they keep their existing user settings. Manually change the settings in the User Setup section. |
| Authentication fails. | Check the Failed Attempts report.<br>The retry interval may be too short. (The default is 5 seconds.) Increase the retry interval (**tacacs-server timeout 20**) on the AAA client to 20 or greater. |
| The AAA client times out when authenticating against a Windows user database. | Increase the TACACS+/RADIUS timeout interval from the default, 5, to 20. Set the Cisco IOS command as follows:<br>**tacacs-server timeout 20**<br>**radius-server timeout 20** |



Downloaded from www.Manualslib.com manuals search engine

| Condition | Recovery Action |
|---|---|
| Authentication fails; the error "Unknown NAS" appears in the Failed Attempts log. | Verify the following:<br>• AAA client is configured under the Network Configuration section.<br>• If you have RADIUS/TACACS source-interface command configured on the AAA client, make sure the client on ACS is configured using the IP address of the interface specified.<br>Alternatively, you can configure a default NAS in the NAS configuration area by leaving the hostname and IP address blank and entering only the key. |
| Authentication fails; the error "key mismatch" appears in the Failed Attempts log. | Verify that the TACACS+ or RADIUS keys, in both AAA client and Cisco Secure ACS, are identical (case sensitive).<br>Re-enter the keys to confirm they are identical. |
| User can authenticate, but authorizations are not what is expected. | Different vendors use different AV pairs. AV pairs used in one vendor protocol may be ignored by another vendor protocol. Make sure that the user settings reflect the correct vendor protocol; for example, RADIUS (Cisco IOS/PIX). |
| LEAP authentication fails; the error "Radius extension DLL rejected user" appears in the Failed Attempts log. | Verify the correct authentication type has been set on the Access Point. Make sure that, at a minimum, the Network-EAP check box is selected<br>If you are using an external user database for authentication, verify that it is supported. For more information, see Authentication Protocol-Database Compatibility, page 1-10. |



Downloaded from www.Manualslib.com manuals search engine

# TACACS+ and RADIUS Attribute Issues

| Condition | Recovery Action |
|---|---|
| TACACS+ and RADIUS attributes do not appear on the Group Setup page. | Make sure that you have at least one RADIUS or TACACS+ AAA client configured in the Network Configuration section and that, in the Interface Configuration section, you have enabled the attributes you need to configure.<br>**Note** Some attributes are not customer-configurable in Cisco Secure ACS; instead, their values are set by Cisco Secure ACS. |



Downloaded from www.Manualslib.com manuals search engine

# TACACS+ Attribute-Value Pairs

Cisco Secure Access Control Server (ACS) for Windows Server supports Terminal Access Controller Access Control System (TACACS+) attribute-value (AV) pairs. You can enable different AV pairs for any supported attribute value.

## Cisco IOS AV Pair Dictionary

Before selecting TACACS+ AV pairs for Cisco Secure ACS, confirm that your AAA client is running Cisco IOS Release 11.2 or later. Earlier versions of Cisco IOS work with Cisco Secure ACS but do not fully support the TACACS+ features in Cisco Secure ACS.

**Note** If you specify a given AV pair in Cisco Secure ACS, you must also enable the corresponding AV pair in the Cisco IOS software running on the AAA client. Therefore, you must consider which AV pairs your Cisco IOS release supports. If Cisco Secure ACS sends an AV pair to the AAA client that the Cisco IOS software does not support, that attribute is not implemented.

For more information on TACACS+ AV pairs, refer to Cisco IOS documentation for the release of Cisco IOS running on your AAA clients.

**Note** All TACACS+ values are strings. The concept of value “type” does not exist in TACACS+ as it does in Remote Access Dial-In User Service (RADIUS).



Downloaded from www.Manualslib.com manuals search engine

# TACACS+ AV Pairs

**Note** Beginning with Cisco Secure ACS 2.3, some TACACS+ attributes no longer appear on the Group Setup page. This is because IP pools and callback supersede the following attributes:

**addr**
**addr-pool**
**callback-dialstring**

Additionally, these attributes cannot be set via database synchronization, and **ip:addr=n.n.n.n** is not allowed as a Cisco vendor-specific attribute (VSA).

Cisco Secure ACS supports many TACACS+ AV pairs. For descriptions of these attributes, refer to Cisco IOS documentation for the release of Cisco IOS running on your AAA clients. TACACS+ AV pairs supported in Cisco Secure ACS are as follows:

- acl=
- addr=
- addr-pool=
- autocmd=
- callback-dialstring
- callback-line
- callback-rotary
- cmd-arg=
- cmd=
- dns-servers=
- gw-password
- idletime=
- inacl#*n*
- inacl=
- interface-config=



Downloaded from www.Manualslib.com manuals search engine

- ip-addresses
- link-compression=
- load-threshold=*n*
- max-links=*n*
- nas-password
- nocallback-verify
- noescape=
- nohangup=
- old-prompts
- outacl#*n*
- outacl=
- pool-def#*n*
- pool-timeout=
- ppp-vj-slot-compression
- priv-lvl=
- protocol=
- route
- route#*n*
- routing=
- rte-ftr-in#*n*
- rte-ftr-out#*n*
- sap#*n*
- sap-fltr-in#*n*
- sap-fltr-out#*n*
- service=
- source-ip=
- timeout=
- tunnel-id



Downloaded from www.Manualslib.com manuals search engine

- wins-servers=
- zonelist=

# TACACS+ Accounting AV Pairs

Cisco Secure ACS supports many TACACS+ accounting AV pairs. For descriptions of these attributes, see Cisco IOS documentation for the release of Cisco IOS running on your AAA clients. TACACS+ accounting AV pairs supported in Cisco Secure ACS are as follows:

- bytes_in
- bytes_out
- cmd
- data-rate
- disc-cause
- disc-cause-ext
- elapsed_time
- event
- mlp-links-max
- mlp-sess-id
- nas-rx-speed
- nas-tx-speed
- paks_in
- paks_out
- port
- pre-bytes-in
- pre-bytes-out
- pre-paks-in
- pre-paks-out
- pre-session-time
- priv_level



Downloaded from www.Manualslib.com manuals search engine

- protocol
- reason
- service
- start_time
- stop_time
- task_id
- timezone
- xmit-rate



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

# RADIUS Attributes

Cisco Secure Access Control Server (ACS) for Windows Server supports many RADIUS attributes. You can enable different attribute-value (AV) pairs for IETF RADIUS and for any supported vendor. This appendix lists the standard attributes, vendor-proprietary attributes, and vendor-specific attributes supported by Cisco Secure ACS.

For outbound attributes, you can configure the attributes sent and their content using the Cisco Secure ACS HTML interface. The RADIUS attributes sent to a AAA client in an access-accept message are user specific. To configure a specific attribute to be sent for a given user, you must ensure the following:

1. In the Network Configuration section, the AAA client entry corresponding to the access device that grants network access to the user must be configured to use a variety of RADIUS that supports the attribute you want sent to the AAA client. For more information about the RADIUS attribute sets supported by RADIUS varieties, see Protocol Configuration Options for RADIUS, page 3-11.
2. In the Interface Configuration section, the attribute must be enabled so that it appears on user or user group profile pages. You can enable attributes on the page corresponding to the RADIUS variety that supports the attribute. For example, IETF RADIUS Session-Timeout attribute (27) appears on the RADIUS (IETF) page.

**Note** By default, per-user RADIUS attributes are not enabled. Before you can enable attributes on a per-user basis, you must enable the Per-user TACACS+/RADIUS Attributes option on the Advanced Options page in the Interface Configuration section.



Downloaded from www.Manualslib.com manuals search engine

3. In the profile you use to control authorizations for the user—either in User Setup or Group Setup—the attribute must be enabled. This causes Cisco Secure ACS to send the attribute to the AAA client in the access-accept message. In the options associated with the attribute, you can determine the value of the attribute sent to the AAA client.

**Note** Settings in a user profile override settings in a group profile. For example, if Session-Timeout is configured in the user profile and also in the group the user is assigned to, Cisco Secure ACS sends the AAA client the Session-Timeout value specified in the user profile.

This chapter contains the following topics:


- Cisco IOS Dictionary of RADIUS AV Pairs, page C-2
- Cisco IOS/PIX Dictionary of RADIUS VSAs, page C-5
- About the cisco-av-pair RADUIS Attribute, page C-7
- Cisco VPN 3000 Concentrator Dictionary of RADIUS VSAs, page C-9
- Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs, page C-13
- Cisco Building Broadband Service Manager Dictionary of RADIUS VSA, page C-14
- IETF Dictionary of RADIUS AV Pairs, page C-14
- Microsoft MPPE Dictionary of RADIUS VSAs, page C-28
- Ascend Dictionary of RADIUS AV Pairs, page C-31
- Nortel Dictionary of RADIUS VSAs, page C-43
- Juniper Dictionary of RADIUS VSAs, page C-44


# Cisco IOS Dictionary of RADIUS AV Pairs

Cisco Secure ACS supports Cisco IOS RADIUS AV pairs. Before selecting AV pairs for Cisco Secure ACS, confirm that your AAA client is a compatible release of Cisco IOS or compatible AAA client software. For more information, see Network and Port Requirements, page 2-4.



Downloaded from www.Manualslib.com manuals search engine

**Note** If you specify a given AV pair on Cisco Secure ACS, the corresponding AV pair must be implemented in the Cisco IOS software running on the network device. Always consider which AV pairs your Cisco IOS release supports. If Cisco Secure ACS sends an AV pair that the Cisco IOS software does not support, the attribute is not implemented.

**Note** Because IP pools and callback supersede them, the following RADIUS attributes do not appear on the Group Setup page:

**8, Framed-IP-Address**
**19, Callback-Number**
**218, Ascend-Assign-IP-Pool**

None of these attributes can be set via RDBMS Synchronization.

Table C-1 lists the supported Cisco IOS RADIUS AV pairs.

***Table C-1 Cisco IOS Software RADIUS AV Pairs***

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 1 | User-Name | String | Inbound | No |
| 2 | User-Password | String | Outbound | No |
| 3 | CHAP-Password | String | Outbound | No |
| 4 | NAS-IP Address | Ipaddr | Inbound | No |
| 5 | NAS-Port | Integer | Inbound | No |
| 6 | Service-Type | Integer | Both | No |
| 7 | Framed-Protocol | Integer | Both | No |
| 9 | Framed-IP-Netmask | Ipaddr (maximum length 15 characters) | Outbound | No |
| 10 | Framed-Routing | Integer | Outbound | No |
| 11 | Filter-Id | String | Outbound | Yes |
| 12 | Framed-MTU | Integer (maximum length 10 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-1 Cisco IOS Software RADIUS AV Pairs (continued)*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 13 | Framed-Compression | Integer | Outbound | Yes |
| 14 | Login-IP-Host | Ipaddr (maximum length 15 characters) | Both | Yes |
| 15 | Login-Service | Integer | Both | No |
| 16 | Login-TCP-Port | Integer (maximum length 10 characters) | Outbound | No |
| 18 | Reply-Message | String | Outbound | Yes |
| 21 | Expiration | Date | — | — |
| 22 | Framed-Route | String | Outbound | Yes |
| 24 | State | String (maximum length 253 characters) | Outbound | No |
| 25 | Class | String | Outbound | Yes |
| 26 | Vendor specific | String | Outbound | Yes |
| 27 | Session-Timeout | Integer (maximum length 10 characters) | Outbound | No |
| 28 | Idle-Timeout | Integer (maximum length 10 characters) | Outbound | No |
| 30 | Called-Station-ID | String | Inbound | No |
| 31 | Calling-Station-ID | String | Inbound | No |
| 33 | Login-LAT-Service | String (maximum length 253 characters) | Inbound | No |
| 40 | Acct-Status-Type | Integer | Inbound | No |
| 41 | Acct-Delay-Time | Integer | Inbound | No |
| 42 | Acct-Input-Octets | Integer | Inbound | No |
| 43 | Acct-Output-Octets | Integer | Inbound | No |
| 44 | Acct-Session-ID | String | Inbound | No |
| 45 | Acct-Authentic | Integer | Inbound | No |
| 46 | Acct-Session-Time | Integer | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-1 Cisco IOS Software RADIUS AV Pairs (continued)*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 47 | Acct-Input-Packets | Integer | Inbound | No |
| 48 | Acct-Output-Packets | Integer | Inbound | No |
| 49 | Acct-Terminate-Cause | Integer | Inbound | No |
| 61 | NAS-Port-Type | Integer | Inbound | No |
| 62 | NAS-Port-Limit | Integer (maximum length 10 characters) | Both | No |

# Cisco IOS/PIX Dictionary of RADIUS VSAs

Cisco Secure ACS supports Cisco IOS/PIX vendor-specific attributes (VSAs). The vendor ID for this Cisco RADIUS Implementation is 9. Table C-2 lists the supported Cisco IOS/PIX RADIUS VSAs.

**Note** For a discussion of the Cisco IOS/PIX RADIUS cisco-av-pair attribute, see About the cisco-av-pair RADUIS Attribute, page C-7.

**Note** For details about the Cisco IOS H.323 VSAs, refer to Cisco IOS Voice-over-IP documentation.

**Note** For details about the Cisco IOS Node Route Processor-Service Selection Gateway VSAs (VSAs 250, 251, and 252), refer to Cisco IOS documentation.

*Table C-2 Cisco IOS/PIX RADIUS VSAs*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 1 | cisco-av-pair | String | Both | Yes |
| 2 | cisco-nas-port | String | Inbound | No |
| 23 | cisco-h323-remote-address | String | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-2 Cisco IOS/PIX RADIUS VSAs (continued)*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 24 | cisco-h323-conf-id | String | Inbound | No |
| 25 | cisco-h323-setup-time | String | Inbound | No |
| 26 | cisco-h323-call-origin | String | Inbound | No |
| 27 | cisco-h323-call-type | String | Inbound | No |
| 28 | cisco-h323-connect-time | String | Inbound | No |
| 29 | cisco-h323-disconnect-time | String | Inbound | No |
| 30 | cisco-h323-disconnect-cause | String | Inbound | No |
| 31 | cisco-h323-voice-quality | String | Inbound | No |
| 33 | cisco-h323-gw-id | String | Inbound | No |
| 35 | cisco-h323-incoming-conn-id | String | Inbound | No |
| 101 | cisco-h323-credit-amount | String (maximum length 247 characters) | Outbound | No |
| 102 | cisco-h323-credit-time | String (maximum length 247 characters) | Outbound | No |
| 103 | cisco-h323-return-code | String (maximum length 247 characters) | Outbound | No |
| 104 | cisco-h323-prompt-id | String (maximum length 247 characters) | Outbound | No |
| 105 | cisco-h323-day-and-time | String (maximum length 247 characters) | Outbound | No |
| 106 | cisco-h323-redirect-number | String (maximum length 247 characters) | Outbound | No |
| 107 | cisco-h323-preferred-lang | String (maximum length 247 characters) | Outbound | No |
| 108 | cisco-h323-redirect-ip-addr | String (maximum length 247 characters) | Outbound | No |
| 109 | cisco-h323-billing-model | String (maximum length 247 characters) | Outbound | No |
| 110 | cisco-h323-currency | String (maximum length 247 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-2 Cisco IOS/PIX RADIUS VSAs (continued)*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 250 | cisco-ssg-account-info | String (maximum length 247 characters) | Outbound | No |
| 251 | cisco-ssg-service-info | String (maximum length 247 characters) | Both | No |
| 253 | cisco-ssg-control-info | String (maximum length 247 characters) | Both | No |

# About the cisco-av-pair RADUIS Attribute

The first attribute in the Cisco IOS/PIX RADIUS implementation, cisco-av-pair, supports the inclusion of many AV pairs, using the following format:

*attribute sep value*

where *attribute* and *value* are an AV pair supported by the releases of IOS implemented on your AAA clients, and *sep* is "=" for mandatory attributes and "*" for optional attributes. This allows the full set of TACACS+ authorization features to be used for RADIUS.

**Note** The attribute name in an AV pair is case sensitive. Typically, attribute names are all in lowercase letters.

The following is an example of two AV pairs included in a single Cisco IOS/PIX RADIUS cisco-av-pair attribute:

```
ip:addr-pool=first
shell:priv-lvl=15
```

The first example causes the Cisco multiple named IP address pools feature to be activated during IP authorization (during PPP IPCP address assignment). The second example causes a user of a device-hosted administrative session to have immediate access to EXEC commands.



Downloaded from www.Manualslib.com manuals search engine

In IOS, support for Network Admission Control (NAC) includes the use of the following AV pairs:

- **url-redirect**—Enables the AAA client to intercept an HTTP request and redirect it to a new URL. This is especially useful if the result of posture validation indicates that the NAC-client computer requires an update or patch that you have made available on a remediation web server. For example, a user can be redirected to a remediation web server to download and apply a new virus DAT file or an operating system patch. For example:

  ```
  url-redirect=http://10.1.1.1
  ```

- **posture-token**—Enables Cisco Secure ACS to send a text version of a system posture token (SPT) derived by posture validation. The SPT is always sent in numeric format and using the posture-token AV pair makes viewing the result of a posture validation request more easily read on the AAA client. For example:

  ```
  posture-token=Healthy
  ```

**Caution** The posture-token AV pair is the only way that Cisco Secure ACS notifies the AAA client of the SPT returned by posture validation. Because you manually configure the posture-token AV pair, errors in configuring posture-token can result in the incorrect system posture token being sent to the AAA client or, if the AV pair name is mistyped, the AAA client not receiving the system posture token at all.

  For a list of valid SPTs, see Posture Tokens, page 14-4.

- **status-query-timeout**—Overrides the status-query default value of the AAA client with the value you specify, in seconds. For example:

  ```
  status-query-timeout=150
  ```

For more information about AV pairs supported by IOS, refer to the documentation for the releases of IOS implemented on your AAA clients.



Downloaded from www.Manualslib.com manuals search engine

# Cisco VPN 3000 Concentrator Dictionary of RADIUS VSAs

Cisco Secure ACS supports Cisco VPN 3000 RADIUS VSAs. The vendor ID for this Cisco RADIUS Implementation is 3076. Table C-3 lists the supported Cisco VPN 3000 Concentrator RADIUS VSAs.

**Note** Some of the RADIUS VSAs supported by Cisco VPN 3000 Concentrators are interdependent. Before you implement them, we recommend that you refer to Cisco VPN 3000-series Concentrator documentation.

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, Cisco Secure ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the Cisco Secure ACS HTML interface or how those attributes might be configured.

*Table C-3 Cisco VPN 3000 Concentrator RADIUS VSAs*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 1 | CVPN3000-Access-Hours | String (maximum length 247 characters) | Outbound | No |
| 2 | CVPN3000-Simultaneous-Logins | Integer (maximum length 10 characters) | Outbound | No |
| 5 | CVPN3000-Primary-DNS | Ipaddr (maximum length 15 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-3 Cisco VPN 3000 Concentrator RADIUS VSAs (continued)*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 6 | CVPN3000-Secondary-DNS | Ipaddr (maximum length 15 characters) | Outbound | No |
| 7 | CVPN3000-Primary-WINS | Ipaddr (maximum length 15 characters) | Outbound | No |
| 8 | CVPN3000-Secondary-WINS | Ipaddr (maximum length 15 characters) | Outbound | No |
| 9 | CVPN3000-SEP-Card-Assignment | Integer | Outbound | No |
| 11 | CVPN3000-Tunneling-Protocols | Integer | Outbound | No |
| 12 | CVPN3000-IPSec-Sec-Association | String (maximum length 247 characters) | Outbound | No |
| 13 | CVPN3000-IPSec-Authentication | Integer | Outbound | No |
| 15 | CVPN3000-IPSec-Banner1 | String (maximum length 247 characters) | Outbound | No |
| 16 | CVPN3000-IPSec-Allow-Passwd-Store | Integer | Outbound | No |
| 17 | CVPN3000-Use-Client-Address | Integer | Outbound | No |
| 20 | CVPN3000-PPTP-Encryption | Integer | Outbound | No |
| 21 | CVPN3000-L2TP-Encryption | Integer | Outbound | No |
| 27 | CVPN3000-IPSec-Split-Tunnel-List | String (maximum length 247 characters) | Outbound | No |
| 28 | CVPN3000-IPSec-Default-Domain | String (maximum length 247 characters) | Outbound | No |
| 29 | CVPN3000-IPSec-Split-DNS-Names | String (maximum length 247 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-3 Cisco VPN 3000 Concentrator RADIUS VSAs (continued)*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 30 | CVPN3000-IPSec-Tunnel-Type | Integer | Outbound | No |
| 31 | CVPN3000-IPSec-Mode-Config | Integer | Outbound | No |
| 33 | CVPN3000-IPSec-User-Group-Lock | Integer | Outbound | No |
| 34 | CVPN3000-IPSec-Over-UDP | Integer | Outbound | No |
| 35 | CVPN3000-IPSec-Over-UDP-Port | Integer (maximum length 10 characters) | Outbound | No |
| 36 | CVPN3000-IPSec-Banner2 | String (maximum length 247 characters) | Outbound | No |
| 37 | CVPN3000-PPTP-MPPC-Compression | Integer | Outbound | No |
| 38 | CVPN3000-L2TP-MPPC-Compression | Integer | Outbound | No |
| 39 | CVPN3000-IPSec-IP-Compression | Integer | Outbound | No |
| 40 | CVPN3000-IPSec-IKE-Peer-ID-Check | Integer | Outbound | No |
| 41 | CVPN3000-IKE-Keep-Alives | Integer | Outbound | No |
| 42 | CVPN3000-IPSec-Auth-On-Rekey | Integer | Outbound | No |
| 45 | CVPN3000-Required-Client-Firewall-Vendor-Code | Integer (maximum length 10 characters) | Outbound | No |
| 46 | CVPN3000-Required-Client-Firewall-Product-Code | Integer (maximum length 10 characters) | Outbound | No |
| 47 | CVPN3000-Required-Client-Firewall-Description | String (maximum length 247 characters) | Outbound | No |
| 48 | CVPN3000-Require-HW-Client-Auth | Integer | Outbound | No |
| 49 | CVPN3000-Require-Individual-User-Auth | Integer | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-3 Cisco VPN 3000 Concentrator RADIUS VSAs (continued)*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 50 | CVPN3000-Authenticated-User-Idle-Timeout | Integer (maximum length 10 characters) | Outbound | No |
| 51 | CVPN3000-Cisco-IP-Phone-Bypass | Integer | Outbound | No |
| 52 | CVPN3000-User-Auth-Server-Name | String (maximum length 247 characters) | Outbound | No |
| 53 | CVPN3000-User-Auth-Server-Port | Integer (maximum length 10 characters) | Outbound | No |
| 54 | CVPN3000-User-Auth-Server-Secret | String (maximum length 247 characters) | Outbound | No |
| 55 | CVPN3000-IPSec-Split-Tunneling-Policy | Integer | Outbound | No |
| 56 | CVPN3000-IPSec-Required-Client-Firewall-Capability | Integer | Outbound | No |
| 57 | CVPN3000-IPSec-Client-Firewall-Filter-Name | String (maximum length 247 characters) | Outbound | No |
| 58 | CVPN3000-IPSec-Client-Firewall-Filter-Optional | Integer | Outbound | No |
| 59 | CVPN3000-IPSec-Backup-Servers | Integer | Outbound | No |
| 60 | CVPN3000-IPSec-Backup-Server-List | String (maximum length 247 characters) | Outbound | No |
| 62 | CVPN3000-MS-Client-Intercept-DHCP-Configure-Message | Integer | Outbound | No |
| 63 | CVPN3000-MS-Client-Subnet-Mask | Ipaddr (maximum length 15 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-3 Cisco VPN 3000 Concentrator RADIUS VSAs (continued)*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 64 | CVPN3000-Allow-Network-Extension-Mode | Integer | Outbound | No |
| 135 | CVPN3000-Strip-Realm | Integer | Outbound | No |

# Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs

Cisco Secure ACS supports the Cisco VPN 5000 RADIUS VSAs. The vendor ID for this Cisco RADIUS Implementation is 255. Table C-4 lists the supported Cisco VPN 5000 Concentrator RADIUS VSAs.

*Table C-4 Cisco VPN 5000 Concentrator RADIUS VSAs*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 001 | CVPN5000-Tunnel-Throughput | Integer | Inbound | No |
| 002 | CVPN5000-Client-Assigned-IP | String | Inbound | No |
| 003 | CVPN5000-Client-Real-IP | String | Inbound | No |
| 004 | CVPN5000-VPN-GroupInfo | String (maximum length 247 characters) | Outbound | No |
| 005 | CVPN5000-VPN-Password | String (maximum length 247 characters) | Outbound | No |
| 006 | CVPN5000-Echo | Integer | Inbound | No |
| 007 | CVPN5000-Client-Assigned-IPX | Integer | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

# Cisco Building Broadband Service Manager Dictionary of RADIUS VSA

Cisco Secure ACS supports a Cisco Building Broadband Service Manager (BBSM) RADIUS VSA. The vendor ID for this Cisco RADIUS Implementation is 5263. Table C-5 lists the supported Cisco BBSM RADIUS VSA.

*Table C-5 Cisco BBSM RADIUS VSA*

| Number | Attribute | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|
| 001 | CBBSM-Bandwidth | Integer | Both | No |

# IETF Dictionary of RADIUS AV Pairs

Table C-6 lists the supported RADIUS (IETF) attributes. If the attribute has a security server-specific format, the format is specified.

*Table C-6 RADIUS (IETF) Attributes*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 1 | User-Name | Name of the user being authenticated. | String | Inbound | No |
| 2 | User-Password | User password or input following an access challenge. Passwords longer than 16 characters are encrypted using IETF Draft #2 or later specifications. | String | Outbound | No |
| 3 | CHAP-Password | PPP (Point-to-Point Protocol) CHAP (Challenge Handshake Authentication Protocol) response to an Access-Challenge. | String | Outbound | No |
| 4 | NAS-IP Address | IP address of the AAA client that is requesting authentication. | Ipaddr | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 5 | NAS-Port | Physical port number of the AAA client that is authenticating the user. The AAA client port value (32 bits) consists of one or two 16-bit values, depending on the setting of the RADIUS server extended **portnames** command. Each 16-bit number is a 5-digit decimal integer interpreted as follows:<br>• For asynchronous terminal lines, async network interfaces, and virtual async interfaces, the value is `00`*ttt*, where *ttt* is the line number or async interface unit number.<br>• For ordinary synchronous network interfaces, the value is `10xxx`.<br>• For channels on a primary-rate ISDN (Integrated Services Digital Network) interface, the value is `2ppcc`.<br>• For channels on a basic rate ISDN interface, the value is `3bb0c`.<br>• For other types of interfaces, the value is `6nnss`. | Integer | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 6 | Service-Type | Type of service requested or type of service to be provided:<br>• In a request:<br>– **Framed**—For known PPP or SLIP (Serial Line Internet Protocol) connection.<br>– **Administrative User**—For **enable** command.<br>• In a response:<br>– **Login**—Make a connection.<br>– **Framed**—Start SLIP or PPP.<br>– **Administrative User**—Start an EXEC or **enable ok**.<br>– **Exec User**—Start an EXEC session. | Integer | Both | No |
| 7 | Framed-Protocol | Framing to be used for framed access. | Integer | Both | No |
| 8 | Framed-IP-Address | Address to be configured for the user. | — | — | — |
| 9 | Framed-IP-Netmask | IP netmask to be configured for the user when the user is a router to a network. This AV results in a static route being added for Framed-IP-Address with the mask specified. | Ipaddr (maximum length 15 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 10 | Framed-Routing | Routing method for the user when the user is a router to a network. Only None and Send and Listen values are supported for this attribute. | Integer | Outbound | No |
| 11 | Filter-Id | Name of the filter list for the user, formatted as follows: %d, %d.in, or %d.out. This attribute is associated with the most recent service-type command. For login and EXEC, use %d or %d.out as the line access list value from 0 to 199. For Framed service, use %d or %d.out as interface output access list and %d.in for input access list. The numbers are self-encoding to the protocol to which they refer. | String | Outbound | Yes |
| 12 | Framed-MTU | Indicates the maximum transmission unit (MTU) that can be configured for the user when the MTU is not negotiated by PPP or some other means. | Integer (maximum length 10 characters) | Outbound | No |
| 13 | Framed-Compression | Compression protocol used for the link. This attribute results in "/compress" being added to the PPP or SLIP autocommand generated during EXEC authorization. Not currently implemented for non-EXEC authorization. | Integer | Outbound | Yes |
| 14 | Login-IP-Host | Host to which the user will connect when the Login-Service attribute is included. | Ipaddr (maximum length 15 characters) | Both | Yes |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 15 | Login-Service | Service that should be used to connect the user to the login host.<br>Service is indicated by a numeric value as follows:<br>• 0: Telnet<br>• 1: Rlogin<br>• 2: TCP-Clear<br>• 3: PortMaster<br>• 4: LAT | Integer | Both | No |
| 16 | Login-TCP-Port | TCP (Transmission Control Protocol) port with which the user is to be connected when the Login-Service attribute is also present. | Integer (maximum length 10 characters) | Outbound | No |
| 18 | Reply-Message | Text to be displayed to the user. | String | Outbound | Yes |
| 19 | Callback-Number | — | String | Outbound | No |
| 20 | Callback-Id | — | String | Outbound | No |
| 22 | Framed-Route | Routing information to be configured for the user on this AAA client. The RADIUS RFC (Request for Comments) format (net/bits [router [metric]]) and the old style dotted mask (net mask [router [metric]]) are supported. If the router field is omitted or 0 (zero), the peer IP address is used. Metrics are ignored. | String | Outbound | Yes |
| 23 | Framed-IPX-Network | — | Integer | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 24 | State | Allows State information to be maintained between the AAA client and the RADIUS server. This attribute is applicable only to CHAP challenges. | String (maximum length 253 characters) | Outbound | No |
| 25 | Class | Arbitrary value that the AAA client includes in all accounting packets for this user if supplied by the RADIUS server. | String | Both | Yes |
| 26 | Vendor-Specific | Carries subattributes known as vendor-specific attributes (VSAs), a feature of RADIUS that allows vendors to support their own extended attributes. Subattributes are identified by IANA-assigned vendor numbers in combination with the vendor-assigned subattribute number. For example, the vendor number for Cisco IOS/PIX RADIUS is 9. The cisco-av-pair VSA is attribute 1 in the set of VSAs related to vendor number 9. | String | Outbound | Yes |
| 27 | Session-Timeout | Maximum number of seconds of service to be provided to the user before the session terminates. This AV becomes the per-user absolute timeout. This attribute is not valid for PPP sessions. | Integer (maximum length 10 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 28 | Idle-Timeout | Maximum number of consecutive seconds of idle connection time allowed to the user before the session terminates. This AV becomes the per-user session-timeout. This attribute is not valid for PPP sessions. | Integer (maximum length 10 characters) | Outbound | No |
| 29 | Termination-Action | — | Integer | Both | No |
| 30 | Called-Station-Id | Allows the AAA client to send the telephone number or other information identifying the AAA client as part of the access-request packet using automatic number identification or similar technology. Different devices provide different identifiers. | String | Inbound | No |
| 31 | Calling-Station-Id | Allows the AAA client to send the telephone number or other information identifying the end-user client into as part of the access-request packet, using DNIS (Dialed Number Identification Server) or similar technology. For example, Cisco Aironet Access Points usually send the MAC address of the end-user client. | String | Inbound | No |
| 32 | NAS-Identifier | — | String | Inbound | No |
| 33 | Proxy-State | Included in proxied RADIUS requests per RADIUS standards. The operation of Cisco Secure ACS does not depend on the contents of this attribute. | String (maximum length 253 characters) | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 34 | Login-LAT-Service | System with which the user is to be connected by local area transport (LAT) protocol. This attribute is only available in the EXEC mode. | String (maximum length 253 characters) | Inbound | No |
| 35 | Login-LAT-Node | — | String | Inbound | No |
| 36 | Login-LAT-Group | — | String | Inbound | No |
| 37 | Framed-AppleTalk-Link | — | Integer | Outbound | No |
| 38 | Framed-AppleTalk-Network | — | Integer | Outbound | Yes |
| 39 | Framed-AppleTalk-Zone | — | String | Out | No |
| 40 | Acct-Status-Type | Specifies whether this accounting-request marks the beginning of the user service (start) or the end (stop). | Integer | Inbound | No |
| 41 | Acct-Delay-Time | Number of seconds the client has been trying to send a particular record. | Integer | Inbound | No |
| 42 | Acct-Input-Octets | Number of octets received from the port while this service is being provided. | Integer | Inbound | No |
| 43 | Acct-Output-Octets | Number of octets sent to the port while this service is being delivered. | Integer | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 44 | Acct-Session-Id | Unique accounting identifier that makes it easy to match start and stop records in a log file. The Acct-Session-Id restarts at 1 each time the router is power cycled or the software is reloaded. Contact Cisco support if this is unsuitable. | String | Inbound | No |
| 44 | Acct-Authentic | Way in which the user was authenticated—by RADIUS, by the AAA client itself, or by another remote authentication protocol. This attribute is set to **radius** for users authenticated by RADIUS; to **remote** for TACACS+ and Kerberos; or to **local** for local, enable, line, and if-needed methods. For all other methods, the attribute is omitted. | Integer | Inbound | No |
| 46 | Acct-Session-Time | Number of seconds the user has been receiving service. | Integer | Inbound | No |
| 47 | Acct-Input-Packets | Number of packets received from the port while this service is being provided to a framed user. | Integer | Inbound | No |
| 48 | Acct-Output-Packets | Number of packets sent to the port while this service is being delivered to a framed user. | Integer | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 49 | Acct-Terminate-Cause | Reports details on why the connection was terminated. Termination causes are indicated by a numeric value as follows:<br>• 1: User request<br>• 2: Lost carrier<br>• 3: Lost service<br>• 4: Idle timeout<br>• 5: Session-timeout<br>• 6: Admin reset<br>• 7: Admin reboot<br>• 8: Port error<br>• 9: AAA client error<br>• 10: AAA client request<br>• 11: AAA client reboot<br>• 12: Port unneeded<br>• 13: Port pre-empted<br>• 14: Port suspended<br>• 15: Service unavailable<br>• 16: Callback<br>• 17: User error<br>• 18: Host request | Integer | Inbound | No |
| 50 | Acct-Multi-Session-Id | — | String | Inbound | No |
| 51 | Acct-Link-Count | — | Integer | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 52 | Acct-Input-Gigawords | — | Integer | Inbound | No |
| 53 | Acct-Output-Gigawords | — | Integer | Inbound | No |
| 55 | Event-Timestamp | — | Date | Inbound | No |
| 60 | CHAP-Challenge | — | String | Inbound | No |
| 61 | NAS-Port-Type | Indicates the type of physical port the AAA client is using to authenticate the user. Physical ports are indicated by a numeric value as follows:<br>• 0: Asynchronous<br>• 1: Synchronous<br>• 2: ISDN-Synchronous<br>• 3: ISDN-Asynchronous (V.120)<br>• 4: ISDN- Asynchronous (V.110)<br>• 5: Virtual | Integer | Inbound | No |
| 62 | Port-Limit | Sets the maximum number of ports to be provided to the user by the network access server. | Integer (maximum length 10 characters) | Both | No |
| 63 | Login-LAT-Port | — | String | Both | No |
| 64 | Tunnel-Type | — | Tagged integer | Both | Yes |
| 65 | Tunnel-Medium-Type | — | Tagged integer | Both | Yes |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 66 | Tunnel-Client-Endpoint | — | tagged string | Both | Yes |
| 67 | Tunnel-Server-Endpoint | — | Tagged string | Both | Yes |
| 68 | Acct-Tunnel-Connection | — | String | Inbound | No |
| 69 | Tunnel-Password | — | tagged string | Both | Yes |
| 70 | ARAP-Password | — | String | Inbound | No |
| 71 | ARAP-Features | — | String | Outbound | No |
| 72 | ARAP-Zone-Access | — | Integer | Outbound | No |
| 73 | ARAP-Security | — | Integer | Inbound | No |
| 74 | ARAP-Security-Data | — | String | Inbound | No |
| 75 | Password-Retry | — | Integer | Internal use only | No |
| 76 | Prompt | — | Integer | Internal use only | No |
| 77 | Connect-Info | — | String | Inbound | No |
| 78 | Configuration-Token | — | String | Internal use only | No |
| 79 | EAP-Message | — | String | Internal use only | No |
| 80 | Message-Authenticator | — | String | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 81 | Tunnel-Private-Group-ID | — | tagged string | Both | Yes |
| 82 | Tunnel-Assignment-ID | — | tagged string | Both | Yes |
| 83 | Tunnel-Preference | — | Tagged integer | Both | No |
| 85 | Acct-Interim-Interval | — | Integer | Outbound | No |
| 87 | NAS-Port-Id | — | String | Inbound | No |
| 88 | Framed-Pool | — | String | Internal use only | No |
| 90 | Tunnel-Client-Auth-ID | — | tagged string | Both | Yes |
| 91 | Tunnel-Server-Auth-ID | — | tagged string | Both | Yes |
| 135 | Primary-DNS-Server | — | Ipaddr | Both | No |
| 136 | Secondary-DNS-Server | — | Ipaddr | Both | No |
| 187 | Multilink-ID | — | Integer | Inbound | No |
| 188 | Num-In-Multilink | — | Integer | Inbound | No |
| 190 | Pre-Input-Octets | — | Integer | Inbound | No |
| 191 | Pre-Output-Octets | — | Integer | Inbound | No |
| 192 | Pre-Input-Packets | — | Integer | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-6 RADIUS (IETF) Attributes (continued)*

| Number | Name | Description | Type of Value | Inbound/Outbound | Multiple |
|---|---|---|---|---|---|
| 193 | Pre-Output-Packets | — | Integer | Inbound | No |
| 194 | Maximum-Time | — | Integer | Both | No |
| 195 | Disconnect-Cause | — | Integer | Inbound | No |
| 197 | Data-Rate | — | Integer | Inbound | No |
| 198 | PreSession-Time | — | Integer | Inbound | No |
| 208 | PW-Lifetime | — | Integer | Outbound | No |
| 209 | IP-Direct | — | Ipaddr | Outbound | No |
| 210 | PPP-VJ-Slot-Comp | — | Integer | Outbound | No |
| 218 | Assign-IP-pool | — | Integer | Outbound | No |
| 228 | Route-IP | — | Integer | Outbound | No |
| 233 | Link-Compression | — | Integer | Outbound | No |
| 234 | Target-Utils | — | Integer | Outbound | No |
| 235 | Maximum-Channels | — | Integer | Outbound | No |
| 242 | Data-Filter | — | Ascend filter | Outbound | Yes |
| 243 | Call-Filter | — | Ascend filter | Outbound | Yes |
| 244 | Idle-Limit | — | Integer | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

# Microsoft MPPE Dictionary of RADIUS VSAs

Cisco Secure ACS supports the Microsoft RADIUS VSAs used for Microsoft Point-to-Point Encryption (MPPE). The vendor ID for this Microsoft RADIUS Implementation is 311. MPPE is an encryption technology developed by Microsoft to encrypt point-to-point (PPP) links. These PPP connections can be via a dial-up line, or over a VPN tunnel such as PPTP. MPPE is supported by several RADIUS network device vendors that Cisco Secure ACS supports. The following Cisco Secure ACS RADIUS protocols support the Microsoft RADIUS VSAs:

- Cisco IOS
- Cisco VPN 3000
- Ascend

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, Cisco Secure ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the Cisco Secure ACS HTML interface or how those attributes might be configured.

Table C-7 lists the supported MPPE RADIUS VSAs.

***Table C-7 Microsoft MPPE RADIUS VSAs***

| Number | Attribute | Type of Value | Description | Inbound/ Outbound | Multiple |
|---|---|---|---|---|---|
| 1 | MS-CHAP-Response | String | — | Inbound | No |
| 2 | MS-CHAP-Error | String | — | Outbound | No |
| 3 | MS-CHAP-CPW-1 | String | — | Inbound | No |
| 4 | MS-CHAP-CPW-2 | String | — | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-7 Microsoft MPPE RADIUS VSAs (continued)*

| Number | Attribute | Type of Value | Description | Inbound/ Outbound | Multiple |
|---|---|---|---|---|---|
| 5 | MS-CHAP-LM-Enc-PW | String | — | Inbound | No |
| 6 | MS-CHAP-NT-Enc-PW | String | — | Inbound | No |
| 7 | MS-MPPE-Encryption-Policy | Integer | The MS-MPPE-Encryption-Policy attribute signifies whether the use of encryption is allowed or required. If the Policy field is equal to 1 (Encryption-Allowed), any or none of the encryption types specified in the MS-MPPE-Encryption-Types attribute can be used. If the Policy field is equal to 2 (Encryption-Required), any of the encryption types specified in the MS-MPPE-Encryption-Types attribute can be used, but at least one must be used. | Outbound | No |
| 8 | MS-MPPE-Encryption-Types | Integer | The MS-MPPE-Encryption-Types attribute signifies the types of encryption available for use with MPPE. It is a four octet integer that is interpreted as a string of bits. | Outbound | No |
| 10 | MS-CHAP-Domain | String | — | Inbound | No |
| 11 | MS-CHAP-Challenge | String | — | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-7 Microsoft MPPE RADIUS VSAs (continued)*

| Number | Attribute | Type of Value | Description | Inbound/ Outbound | Multiple |
|---|---|---|---|---|---|
| 12 | MS-CHAP-MPPE-Keys | String | The MS-CHAP-MPPE-Keys attribute contains two session keys for use by the MPPE. This attribute is only included in Access-Accept packets.<br>**Note** The MS-CHAP-MPPE-Keys attribute value is autogenerated by Cisco Secure ACS; there is no value to set in the HTML interface. | Outbound | No |
| 16 | MS-MPPE-Send-Key | String (maximum length 240 characters) | The MS-MPPE-Send-Key attribute contains a session key for use by MPPE. This key is for encrypting packets sent from the AAA client to the remote host. This attribute is only included in Access-Accept packets. | Outbound | No |
| 17 | MS-MPPE-Recv-Key | String (maximum length 240 characters) | The MS-MPPE-Recv-Key attribute contains a session key for use by MPPE. This key is for encrypting packets received by the AAA client from the remote host. This attribute is only included in Access-Accept packets. | Outbound | No |
| 18 | MS-RAS-Version | String | — | Inbound | No |
| 25 | MS-CHAP-NT-Enc-PW | String | — | Inbound | No |
| 26 | MS-CHAP2-Response | String | — | Outbound | No |
| 27 | MS-CHAP2-CPW | String | — | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

# Ascend Dictionary of RADIUS AV Pairs

Cisco Secure ACS supports the Ascend RADIUS AV pairs. Table C-8 contains Ascend RADIUS dictionary translations for parsing requests and generating responses. All transactions are composed of AV pairs. The value of each attribute is specified as one of the following valid data types:

- **String**—0-253 octets.
- **Abinary**—0-254 octets.
- **Ipaddr**—4 octets in network byte order.
- **Integer**—32-bit value in big endian order (high byte first).
- **Call filter**—Defines a call filter for the profile.

**Note** RADIUS filters are retrieved only when a call is placed using a RADIUS outgoing profile or answered using a RADIUS incoming profile. Filter entries are applied in the order in which they are entered. If you make changes to a filter in an Ascend RADIUS profile, the changes do not take effect until a call uses that profile.

- **Date**—32-bit value in big-endian order. For example, seconds since 00:00:00 universal time (UT), January 1, 1970.
- **Enum**—Enumerated values are stored in the user file with dictionary value translations for easy administration.

*Table C-8 Ascend RADIUS Attributes*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| **Dictionary of Ascend Attributes** | | | | |
| 1 | User-Name | String | Inbound | No |
| 2 | User-Password | String | Outbound | No |
| 3 | CHAP-Password | String | Outbound | No |
| 4 | NAS-IP-Address | Ipaddr | Inbound | No |
| 5 | NAS-Port | Integer | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 6 | Service-Type | Integer | Both | No |
| 7 | Framed-Protocol | Integer | Both | No |
| 8 | Framed-IP-Address | Ipaddr | Both | No |
| 9 | Framed-IP-Netmask | Ipaddr | Outbound | No |
| 10 | Framed-Routing | Integer | Outbound | No |
| 11 | Framed-Filter | String | Outbound | Yes |
| 12 | Framed-MTU | Integer | Outbound | No |
| 13 | Framed-Compression | Integer | Outbound | Yes |
| 14 | Login-IP-Host | Ipaddr | Both | Yes |
| 15 | Login-Service | Integer | Both | No |
| 16 | Login-TCP-Port | Integer | Outbound | No |
| 17 | Change-Password | String | — | — |
| 18 | Reply-Message | String | Outbound | Yes |
| 19 | Callback-ID | String | Outbound | No |
| 20 | Callback-Name | String | Outbound | No |
| 22 | Framed-Route | String | Outbound | Yes |
| 23 | Framed-IPX-Network | Integer | Outbound | No |
| 24 | State | String | Outbound | No |
| 25 | Class | String | Outbound | Yes |
| 26 | Vendor-Specific | String | Outbound | Yes |
| 30 | Call-Station-ID | String | Inbound | No |
| 31 | Calling-Station-ID | String | Inbound | No |
| 40 | Acct-Status-Type | Integer | Inbound | No |
| 41 | Acct-Delay-Time | Integer | Inbound | No |
| 42 | Acct-Input-Octets | Integer | Inbound | No |
| 43 | Acct-Output-Octets | Integer | Inbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 44 | Acct-Session-Id | Integer | Inbound | No |
| 45 | Acct-Authentic | Integer | Inbound | No |
| 46 | Acct-Session-Time | Integer | Inbound | No |
| 47 | Acct-Input-Packets | Integer | Inbound | No |
| 48 | Acct-Output-Packets | Integer | Inbound | No |
| 64 | Tunnel-Type | String | Both | Yes |
| 65 | Tunnel-Medium-Type | String | Both | Yes |
| 66 | Tunnel-Client-Endpoint | String (maximum length 250 characters) | Both | Yes |
| 67 | Tunnel-Server-Endpoint | String (maximum length 250 characters) | Both | Yes |
| 68 | Acct-Tunnel-Connection | Integer (maximum length 253 characters) | Inbound | No |
| 104 | Ascend-Private-Route | String (maximum length 253 characters) | Both | No |
| 105 | Ascend-Numbering-Plan-ID | Integer (maximum length 10 characters) | Both | No |
| 106 | Ascend-FR-Link-Status-Dlci | Integer (maximum length 10 characters) | Both | No |
| 107 | Ascend-Calling-Subaddress | String (maximum length 253 characters) | Both | No |
| 108 | Ascend-Callback-Delay | String (maximum length 10 characters) | Both | No |
| 109 | Ascend-Endpoint-Disc | String (maximum length 253 characters) | Both | No |
| 110 | Ascend-Remote-FW | String (maximum length 253 characters) | Both | No |
| 111 | Ascend-Multicast-GLeave-Delay | Integer (maximum length 10 characters) | Both | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 112 | Ascend-CBCP-Enable | String | Both | No |
| 113 | Ascend-CBCP-Mode | String | Both | No |
| 114 | Ascend-CBCP-Delay | String (maximum length 10 characters) | Both | No |
| 115 | Ascend-CBCP-Trunk-Group | String (maximum length 10 characters) | Both | No |
| 116 | Ascend-AppleTalk-Route | String (maximum length 253 characters) | Both | No |
| 117 | Ascend-AppleTalk-Peer-Mode | String (maximum length 10 characters) | Both | No |
| 118 | Ascend-Route-AppleTalk | String (maximum length 10 characters) | Both | No |
| 119 | Ascend-FCP-Parameter | String (maximum length 253 characters) | Both | No |
| 120 | Ascend-Modem-PortNo | Integer (maximum length 10 characters) | Inbound | No |
| 121 | Ascend-Modem-SlotNo | Integer (maximum length 10 characters) | Inbound | No |
| 122 | Ascend-Modem-ShelfNo | Integer (maximum length 10 characters) | Inbound | No |
| 123 | Ascend-Call-Attempt-Limit | Integer (maximum length 10 characters) | Both | No |
| 124 | Ascend-Call-Block_Duration | Integer (maximum length 10 characters) | Both | No |
| 125 | Ascend-Maximum-Call-Duration | Integer (maximum length 10 characters) | Both | No |
| 126 | Ascend-Router-Preference | String (maximum length 10 characters) | Both | No |
| 127 | Ascend-Tunneling-Protocol | String (maximum length 10 characters) | Both | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 128 | Ascend-Shared-Profile-Enable | Integer | Both | No |
| 129 | Ascend-Primary-Home-Agent | String (maximum length 253 characters) | Both | No |
| 130 | Ascend-Secondary-Home-Agent | String (maximum length 253 characters) | Both | No |
| 131 | Ascend-Dialout-Allowed | Integer | Both | No |
| 133 | Ascend-BACP-Enable | Integer | Both | No |
| 134 | Ascend-DHCP-Maximum-Leases | Integer (maximum length 10 characters) | Both | No |
| 135 | Ascend-Client-Primary-DNS | Address (maximum length 15 characters) | Both | No |
| 136 | Ascend-Client-Secondary-DNS | Address (maximum length 15 characters) | Both | No |
| 137 | Ascend-Client-Assign-DNS | Enum | Both | No |
| 138 | Ascend-User-Acct-Type | Enum | Both | No |
| 139 | Ascend-User-Acct-Host | Address (maximum length 15 characters) | Both | No |
| 140 | Ascend-User-Acct-Port | Integer (maximum length 10 characters) | Both | No |
| 141 | Ascend-User-Acct-Key | String (maximum length 253 characters) | Both | No |
| 142 | Ascend-User-Acct-Base | Enum (maximum length 10 characters) | Both | No |
| 143 | Ascend-User-Acct-Time | Integer (maximum length 10 characters) | Both | No |
| **Support IP Address Allocation from Global Pools** | | | | |
| 144 | Ascend-Assign-IP-Client | Ipaddr (maximum length 15 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 145 | Ascend-Assign-IP-Server | Ipaddr (maximum length 15 characters) | Outbound | No |
| 146 | Ascend-Assign-IP-Global-Pool | String (maximum length 253 characters) | Outbound | No |
| **DHCP Server Functions** | | | | |
| 147 | Ascend-DHCP-Reply | Integer | Outbound | No |
| 148 | Ascend-DHCP-Pool-Number | Integer (maximum length 10 characters) | Outbound | No |
| **Connection Profile/Telco Option** | | | | |
| 149 | Ascend-Expect-Callback | Integer | Outbound | No |
| **Event Type for an Ascend-Event Packet** | | | | |
| 150 | Ascend-Event-Type | Integer (maximum length 10 characters) | Inbound | No |
| **RADIUS Server Session Key** | | | | |
| 151 | Ascend-Session-Svr-Key | String (maximum length 253 characters) | Outbound | No |
| **Multicast Rate Limit Per Client** | | | | |
| 152 | Ascend-Multicast-Rate-Limit | Integer (maximum length 10 characters) | Outbound | No |
| **Connection Profile Fields to Support Interface-Based Routing** | | | | |
| 153 | Ascend-IF-Netmask | Ipaddr (maximum length 15 characters) | Outbound | No |
| 154 | Ascend-Remote-Addr | Ipaddr (maximum length 15 characters) | Outbound | No |
| **Multicast Support** | | | | |
| 155 | Ascend-Multicast-Client | Integer (maximum length 10 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| **Frame Datalink Profiles** | | | | |
| 156 | Ascend-FR-Circuit-Name | String (maximum length 253 characters) | Outbound | No |
| 157 | Ascend-FR-LinkUp | Integer (maximum length 10 characters) | Outbound | No |
| 158 | Ascend-FR-Nailed-Group | Integer (maximum length 10 characters) | Outbound | No |
| 159 | Ascend-FR-Type | Integer (maximum length 10 characters) | Outbound | No |
| 160 | Ascend-FR-Link-Mgt | Integer (maximum length 10 characters) | Outbound | No |
| 161 | Ascend-FR-N391 | Integer (maximum length 10 characters) | Outbound | No |
| 162 | Ascend-FR-DCE-N392 | Integer (maximum length 10 characters) | Outbound | No |
| 163 | Ascend-FR-DTE-N392 | Integer (maximum length 10 characters) | Outbound | No |
| 164 | Ascend-FR-DCE-N393 | Integer (maximum length 10 characters) | Outbound | No |
| 165 | Ascend-FR-DTE-N393 | Integer (maximum length 10 characters) | Outbound | No |
| 166 | Ascend-FR-T391 | Integer (maximum length 10 characters) | Outbound | No |
| 167 | Ascend-FR-T392 | Integer (maximum length 10 characters) | Outbound | No |
| 168 | Ascend-Bridge-Address | String (maximum length 253 characters) | Outbound | No |
| 169 | Ascend-TS-Idle-Limit | Integer (maximum length 10 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 170 | Ascend-TS-Idle-Mode | Integer (maximum length 10 characters) | Outbound | No |
| 171 | Ascend-DBA-Monitor | Integer (maximum length 10 characters) | Outbound | No |
| 172 | Ascend-Base-Channel-Count | Integer (maximum length 10 characters) | Outbound | No |
| 173 | Ascend-Minimum-Channels | Integer (maximum length 10 characters) | Outbound | No |
| **IPX Static Routes** | | | | |
| 174 | Ascend-IPX-Route | String (maximum length 253 characters) | Inbound | No |
| 175 | Ascend-FT1-Caller | Integer (maximum length 10 characters) | Inbound | No |
| 176 | Ascend-Backup | String (maximum length 253 characters) | Inbound | No |
| 177 | Ascend-Call-Type | Integer | Inbound | No |
| 178 | Ascend-Group | String (maximum length 253 characters) | Inbound | No |
| 179 | Ascend-FR-DLCI | Integer (maximum length 10 characters) | Inbound | No |
| 180 | Ascend-FR-Profile-Name | String (maximum length 253 characters) | Inbound | No |
| 181 | Ascend-Ara-PW | String (maximum length 253 characters) | Inbound | No |
| 182 | Ascend-IPX-Node-Addr | String (maximum length 253 characters) | Both | No |
| 183 | Ascend-Home-Agent-IP-Addr | Ipaddr (maximum length 15 characters) | Outbound | No |
| 184 | Ascend-Home-Agent-Password | String (maximum length 253 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 185 | Ascend-Home-Network-Name | String (maximum length 253 characters) | Outbound | No |
| 186 | Ascend-Home-Agent-UDP-Port | Integer (maximum length 10 characters) | Outbound | No |
| 187 | Ascend-Multilink-ID | Integer | Inbound | No |
| 188 | Ascend-Num-In-Multilink | Integer | Inbound | No |
| 189 | Ascend-First-Dest | Ipaddr | Inbound | No |
| 190 | Ascend-Pre-Input-Octets | Integer | Inbound | No |
| 191 | Ascend-Pre-Output-Octets | Integer | Inbound | No |
| 192 | Ascend-Pre-Input-Packets | Integer | Inbound | No |
| 193 | Ascend-Pre-Output-Packets | Integer | Inbound | No |
| 194 | Ascend-Maximum-Time | Integer (maximum length 10 characters) | Both | No |
| 195 | Ascend-Disconnect-Cause | Integer | Inbound | No |
| 196 | Ascend-Connect-Progress | Integer | Inbound | No |
| 197 | Ascend-Data-Rate | Integer | Inbound | No |
| 198 | Ascend-PreSession-Time | Integer | Inbound | No |
| 199 | Ascend-Token-Idle | Integer (maximum length 10 characters) | Outbound | No |
| 200 | Ascend-Token-Immediate | Integer | Outbound | No |
| 201 | Ascend-Require-Auth | Integer (maximum length 10 characters) | Outbound | No |
| 202 | Ascend-Number-Sessions | String (maximum length 253 characters) | Outbound | No |
| 203 | Ascend-Authen-Alias | String (maximum length 253 characters) | Outbound | No |
| 204 | Ascend-Token-Expiry | Integer (maximum length 10 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 205 | Ascend-Menu-Selector | String (maximum length 253 characters) | Outbound | No |
| 206 | Ascend-Menu-Item | String | Outbound | Yes |
| **RADIUS Password Expiration Options** | | | | |
| 207 | Ascend-PW-Warntime | Integer (maximum length 10 characters) | Outbound | No |
| 208 | Ascend-PW-Lifetime | Integer (maximum length 10 characters) | Outbound | No |
| 209 | Ascend-IP-Direct | Ipaddr (maximum length 15 characters) | Outbound | No |
| 210 | Ascend-PPP-VJ-Slot-Comp | Integer (maximum length 10 characters) | Outbound | No |
| 211 | Ascend-PPP-VJ-1172 | Integer (maximum length 10 characters) | Outbound | No |
| 212 | Ascend-PPP-Async-Map | Integer (maximum length 10 characters) | Outbound | No |
| 213 | Ascend-Third-Prompt | String (maximum length 253 characters) | Outbound | No |
| 214 | Ascend-Send-Secret | String (maximum length 253 characters) | Outbound | No |
| 215 | Ascend-Receive-Secret | String (maximum length 253 characters) | Outbound | No |
| 216 | Ascend-IPX-Peer-Mode | Integer | Outbound | No |
| 217 | Ascend-IP-Pool-Definition | String (maximum length 253 characters) | Outbound | No |
| 218 | Ascend-Assign-IP-Pool | Integer | Outbound | No |
| 219 | Ascend-FR-Direct | Integer | Outbound | No |
| 220 | Ascend-FR-Direct-Profile | String (maximum length 253 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 221 | Ascend-FR-Direct-DLCI | Integer (maximum length 10 characters) | Outbound | No |
| 222 | Ascend-Handle-IPX | Integer | Outbound | No |
| 223 | Ascend-Netware-Timeout | Integer (maximum length 10 characters) | Outbound | No |
| 224 | Ascend-IPX-Alias | String (maximum length 253 characters) | Outbound | No |
| 225 | Ascend-Metric | Integer (maximum length 10 characters) | Outbound | No |
| 226 | Ascend-PRI-Number-Type | Integer | Outbound | No |
| 227 | Ascend-Dial-Number | String (maximum length 253 characters) | Outbound | No |
| **Connection Profile/PPP Options** | | | | |
| 228 | Ascend-Route-IP | Integer | Outbound | No |
| 229 | Ascend-Route-IPX | Integer | Outbound | No |
| 230 | Ascend-Bridge | Integer | Outbound | No |
| 231 | Ascend-Send-Auth | Integer | Outbound | No |
| 232 | Ascend-Send-Passwd | String (maximum length 253 characters) | Outbound | No |
| 233 | Ascend-Link-Compression | Integer | Outbound | No |
| 234 | Ascend-Target-Util | Integer (maximum length 10 characters) | Outbound | No |
| 235 | Ascend-Max-Channels | Integer (maximum length 10 characters) | Outbound | No |
| 236 | Ascend-Inc-Channel-Count | Integer (maximum length 10 characters) | Outbound | No |
| 237 | Ascend-Dec-Channel-Count | Integer (maximum length 10 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 238 | Ascend-Seconds-Of-History | Integer (maximum length 10 characters) | Outbound | No |
| 239 | Ascend-History-Weigh-Type | Integer | Outbound | No |
| 240 | Ascend-Add-Seconds | Integer (maximum length 10 characters) | Outbound | No |
| 241 | Ascend-Remove-Seconds | Integer (maximum length 10 characters) | Outbound | No |
| **Connection Profile/Session Options** | | | | |
| 242 | Ascend-Data-Filter | Call filter | Outbound | Yes |
| 243 | Ascend-Call-Filter | Call filter | Outbound | Yes |
| 244 | Ascend-Idle-Limit | Integer (maximum length 10 characters) | Outbound | No |
| 245 | Ascend-Preempt-Limit | Integer (maximum length 10 characters) | Outbound | No |
| **Connection Profile/Telco Options** | | | | |
| 246 | Ascend-Callback | Integer | Outbound | No |
| 247 | Ascend-Data-Svc | Integer | Outbound | No |
| 248 | Ascend-Force-56 | Integer | Outbound | No |
| 249 | Ascend-Billing-Number | String (maximum length 253 characters) | Outbound | No |
| 250 | Ascend-Call-By-Call | Integer (maximum length 10 characters) | Outbound | No |
| 251 | Ascend-Transit-Number | String (maximum length 253 characters) | Outbound | No |
| **Terminal Server Attributes** | | | | |
| 252 | Ascend-Host-Info | String (maximum length 253 characters) | Outbound | No |
| **PPP Local Address Attribute** | | | | |



Downloaded from www.Manualslib.com manuals search engine

*Table C-8 Ascend RADIUS Attributes (continued)*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 253 | Ascend-PPP-Address | Ipaddr (maximum length 15 characters) | Outbound | No |
| **MPP Percent Idle Attribute** | | | | |
| 254 | Ascend-MPP-Idle-Percent | Integer (maximum length 10 characters) | Outbound | No |
| 255 | Ascend-Xmit-Rate | Integer (maximum length 10 characters) | Outbound | No |

# Nortel Dictionary of RADIUS VSAs

Table C-9 lists the Nortel RADIUS VSAs supported by Cisco Secure ACS. The Nortel vendor ID number is 1584.

*Table C-9 Nortel RADIUS VSAs*

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 035 | Bay-Local-IP-Address | Ipaddr (maximum length 15 characters) | Outbound | No |
| 054 | Bay-Primary-DNS-Server | Ipaddr (maximum length 15 characters) | Outbound | No |
| 055 | Bay-Secondary-DNS-Server | Ipaddr (maximum length 15 characters) | Outbound | No |
| 056 | Bay-Primary-NBNS-Server | Ipaddr (maximum length 15 characters) | Outbound | No |
| 057 | Bay-Secondary-NBNS-Server | Ipaddr (maximum length 15 characters) | Outbound | No |
| 100 | Bay-User-Level | Integer | Outbound | No |
| 101 | Bay-Audit-Level | Integer | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

# Juniper Dictionary of RADIUS VSAs

Table C-10 lists the Juniper RADIUS VSAs supported by Cisco Secure ACS. The Juniper vendor ID number is 2636.

***Table C-10 Juniper RADIUS VSAs***

| Number | Attribute | Type of Value | Inbound/ Outbound | Multiple |
|---|---|---|---|---|
| 001 | Juniper-Local-User-Name | String (maximum length 247 characters) | Outbound | No |
| 002 | Juniper-Allow-Commands | String (maximum length 247 characters) | Outbound | No |
| 003 | Juniper-Deny-Commands | String (maximum length 247 characters) | Outbound | No |



Downloaded from www.Manualslib.com manuals search engine

# CSUtil Database Utility

This appendix details the Cisco Secure Access Control Server (ACS) for Windows Server command-line utility, CSUtil.exe. Among its several functions, CSUtil.exe enables you to add, change, and delete users from a colon-delimited text file. You can also use the utility to add and delete AAA client configurations.

**Note** You can accomplish similar tasks using the ACS System Backup, ACS System Restore, Database Replication, and RDBMS Synchronization features. For more information on these features, see Chapter 9, "System Configuration: Advanced".

This chapter contains the following topics:


- Location of CSUtil.exe and Related Files, page D-2
- CSUtil.exe Syntax, page D-2
- CSUtil.exe Options, page D-3
- Displaying Command-Line Syntax, page D-5
- Backing Up Cisco Secure ACS with CSUtil.exe, page D-6
- Restoring Cisco Secure ACS with CSUtil.exe, page D-7
- Creating a CiscoSecure User Database, page D-8
- Creating a Cisco Secure ACS Database Dump File, page D-10
- Loading the Cisco Secure ACS Database from a Dump File, page D-11
- Compacting the CiscoSecure User Database, page D-12
- User and AAA Client Import Option, page D-14




Downloaded from www.Manualslib.com manuals search engine

- Exporting User List to a Text File, page D-24
- Exporting Group Information to a Text File, page D-25
- Exporting Registry Information to a Text File, page D-26
- Decoding Error Numbers, page D-27
- Recalculating CRC Values, page D-28
- User-Defined RADIUS Vendors and VSA Sets, page D-28
- PAC File Generation, page D-40
- Posture Validation Attributes, page D-44


# Location of CSUtil.exe and Related Files

When you install Cisco Secure ACS in the default location, CSUtil.exe is located in the following directory:

`C:\Program Files\CiscoSecure ACS v`*X.X*`\Utils`

where *X.X* is the version of your Cisco Secure ACS software. Regardless of where you install Cisco Secure ACS, CSUtil.exe is located in the `Utils` directory.

Files generated by or accessed by `CSUtil.exe` are also located in the `Utils` directory.

# CSUtil.exe Syntax

The syntax for the CSUtil.exe command is as follows:

`CSUtil.exe [-q] [-c] [-d] [-g] [-i` *filename*`] [[-p] -l` *filename*`] [-e -`*number*`]`
`[-b` *filename*`] [-r` *filename*`] [-f] [-n] [-u] [-x] [-y] [-listUDV] [-addUDV` *slot filename*`]`
`[-delUDV slot] [-t -filepath` *full filepath*`] [-passwd` *password*`] {-a | -g` *group number* `|`
`-u` *username* `| -f` *user list filepath*`}] [-addAVP` *filename*`]`
`[-delAVP` *vendor-ID application-ID attribute-ID*`] [-dumpAVP` *filename*`]`



Downloaded from www.Manualslib.com manuals search engine

**Note** Most CSUtil.exe options require that you stop the CSAuth service. While the CSAuth service is stopped, Cisco Secure ACS does not authenticate users. To determine if an option requires that you stop CSAuth, refer to the detailed topics about the option. For a list of options and references to the detailed topics about each option, see CSUtil.exe Options, page D-3.

You can combine many of the options in a single use of CSUtil.exe. If you are new to using CSUtil.exe, we recommend performing only one option at a time, with the exception of those options, such as -p, that must be used in conjunction with other options.

Experienced CSUtil.exe users may find it useful to combine CSUtil.exe options, such as in the following example, which would first import AAA client configurations and then generate a dump of all Cisco Secure ACS internal data:

```
CSUtil.exe -i newnases.txt -d
```

# CSUtil.exe Options

CSUtil.exe can perform several actions. The options, listed below in alphabetical order, are detailed in later sections of this chapter.

- **-b**—Backup system to a specified filename. For more information about this option, see Backing Up Cisco Secure ACS with CSUtil.exe, page D-6.
- **-c**—Recalculate database CRC values. For more information about this option, see Recalculating CRC Values, page D-28.
- **-d**—Export all Cisco Secure ACS internal data to a file named `dump.txt`. Using this option requires that you stop the CSAuth service. For more information about this option, see Creating a Cisco Secure ACS Database Dump File, page D-10.
- **-e**—Decode internal Cisco Secure ACS error numbers to ASCII message. For more information about this option, see Decoding Error Numbers, page D-27.
- **-g**—Export group information to a file named `groups.txt`. Using this option requires that you stop the CSAuth service. For more information about this option, see Exporting Group Information to a Text File, page D-25.



Downloaded from www.Manualslib.com manuals search engine

- **-i**—Import user or AAA client information from a file named `import.txt` or a specified file. For more information about this option, see Importing User and AAA Client Information, page D-15.
- **-l**—Load all Cisco Secure ACS internal data from a file named `dump.txt` or named file. Using this option requires that you stop the CSAuth service. For more information about this option, see Loading the Cisco Secure ACS Database from a Dump File, page D-11.
- **-n**—Create CiscoSecure user database and index. Using this option requires that you stop the CSAuth service. For more information about this option, see Creating a CiscoSecure User Database, page D-8.
- **-p**—Reset password aging counters during database load, to be used only in conjunction with the -l option. For more information about this option, see Loading the Cisco Secure ACS Database from a Dump File, page D-11.
- **-q**—Run CSUtil.exe without confirmation prompts.
- **-r**—Restore system from a specified backup filename. For more information about this option, see Restoring Cisco Secure ACS with CSUtil.exe, page D-7.
- **-t**—Generate PAC files for EAP-FAST end-user clients. For more information about this option, see PAC File Generation, page D-40.
- **-u**—Export user information, sorted by group membership, to a file named `users.txt`. Using this option requires that you stop the CSAuth service. For more information about this option, see Exporting User List to a Text File, page D-24.
- **-x**—Display command-line syntax. For more information about this option, see Displaying Command-Line Syntax, page D-5.
- **-y**—Dump Windows Registry configuration information to a file named `setup.txt`. For more information about this option, see Exporting Registry Information to a Text File, page D-26.
- **-addUDV**—Add a user-defined RADIUS vendor-specific attribute (VSA). For more information about this option, see Adding a Custom RADIUS Vendor and VSA Set, page D-29.
- **-delUDV**—Delete a user-defined RADIUS VSA. For more information about this option, see Deleting a Custom RADIUS Vendor and VSA Set, page D-31.



Downloaded from www.Manualslib.com manuals search engine

- **-listUDV**—List all user-defined RADIUS VSAs currently defined in Cisco Secure ACS. For more information about this option, see Listing Custom RADIUS Vendors, page D-32.
- **-addAVP**—Add or modify a posture validation attribute. For more information about this option, see Importing Posture Validation Attribute Definitions, page D-49.
- **-delAVP**—Delete a posture validation attribute. For more information about this option, see Deleting a Posture Validation Attribute Definition, page D-51.
- **-dumpAVP**—Export all posture validation attributes. For more information about this option, see Exporting Posture Validation Attribute Definitions, page D-48.

# Displaying Command-Line Syntax

CSUtil.exe displays command-line syntax for any one of the following reasons:

- The -x option is included in the CSUtil.exe command.
- No options are included with the CSUtil.exe command.
- Incorrect syntax is used with the CSUtil.exe command.

For more information about CSUtil.exe syntax, see CSUtil.exe Syntax, page D-2.

To display command-line syntax for CSUtil.exe, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

**Step 2** Type:

```
CSUtil.exe -x
```

Press **Enter**.

CSUtil.exe displays its command-line syntax.



Downloaded from www.Manualslib.com manuals search engine

# Backing Up Cisco Secure ACS with CSUtil.exe

You can use the -b option to create a system backup of all Cisco Secure ACS internal data. The resulting backup file has the same data as the backup files produced by the ACS Backup feature found in the HTML interface. For more information about the ACS Backup feature, see Cisco Secure ACS Backup, page 8-9.

**Note** During the backup, all services are automatically stopped and restarted. No users are authenticated while the backup is occurring.

To back up Cisco Secure ACS with CSUtil.exe, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

**Step 2** Type:

`CSUtil.exe -b` *filename*

where *filename* is the name of the backup file. Press **Enter**.

CSUtil.exe displays a confirmation prompt.

**Step 3** To confirm that you want to perform a backup and to halt all Cisco Secure ACS services during the backup, type **Y** and press **Enter**.

CSUtil.exe generates a complete backup of all Cisco Secure ACS internal data, including user accounts and system configuration. This process may take a few minutes.

**Note** CSUtil.exe displays the error message “Backup Failed” when it attempts to back up components of Cisco Secure ACS that are empty, such as when no administrator accounts exist. These apply only to components that are empty, not to the overall success or failure of the backup.



Downloaded from www.Manualslib.com manuals search engine

# Restoring Cisco Secure ACS with CSUtil.exe

You can use the -r option to restore all Cisco Secure ACS internal data. The backup file from which you restore Cisco Secure ACS can be one generated by the CSUtil.exe -b option or by the ACS Backup feature in the HTML interface.

Cisco Secure ACS backup files contain two types of data:

- User and group data.
- System configuration.

You can restore either user and group data or system configuration, or both. For more information about the ACS Backup feature, see Cisco Secure ACS Backup, page 8-9.

**Note** During the restoration, all services are automatically stopped and restarted. No users are authenticated while the restoration is occurring.

To restore Cisco Secure ACS with CSUtil.exe, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

**Step 2** Perform one of the following:

- To restore all data (user and group data, and system configuration), type:

  `CSUtil.exe -r all` *filename*

  where *filename* is the name of the backup file. Press **Enter**.

- To restore only user and group data, type:

  `CSUtil.exe -r users` *filename*

  where *filename* is the name of the backup file. Press **Enter**.



Downloaded from www.Manualslib.com manuals search engine

- To restore only the system configuration, type:

  `CSUtil.exe -r config` *filename*

  where *filename* is the name of the backup file. Press **Enter**.

CSUtil.exe displays a confirmation prompt.

**Step 3** To confirm that you want to perform a restoration and to halt all Cisco Secure ACS services during the restoration, type **Y** and press **Enter**.

CSUtil.exe restores the specified portions of your Cisco Secure ACS data. This process may take a few minutes.

**Note** If the backup file is missing a database component, CSUtil.exe displays an error message. Such an error message applies only to the restoration of the missing component. The absence of a database component in a backup is usually intentional and indicates that the component was empty in Cisco Secure ACS at the time the backup was created.

# Creating a CiscoSecure User Database

You can use the -n option to create a CiscoSecure user database.

**Note** Using the -n option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

**Caution** Using the -n option erases all user information in the CiscoSecure user database. Unless you have a current backup or dump of your CiscoSecure user database, all user accounts are lost when you use this option.



Downloaded from www.Manualslib.com manuals search engine

To create a CiscoSecure user database, follow these steps:

**Step 1** If you have not performed a backup or dump of the CiscoSecure user database, do so now before proceeding. For more information about backing up the database, see Backing Up Cisco Secure ACS with CSUtil.exe, page D-6. For more information about performing a dump of the database, see Creating a Cisco Secure ACS Database Dump File, page D-10.

**Step 2** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

**Step 3** If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

The CSAuth service stops.

**Step 4** Type:

```
CSUtil.exe -n
```

and press **Enter**.

CSUtil.exe displays a confirmation prompt.

**Step 5** To confirm that you want to initialize the CiscoSecure user database, type **Y** and press **Enter**.

The CiscoSecure user database is initialized. This process may take a few minutes.

**Step 6** To resume user authentication, type:

```
net start csauth
```

and press **Enter**.



Downloaded from www.Manualslib.com manuals search engine

# Creating a Cisco Secure ACS Database Dump File

You can use the -d option to dump all contents of the CiscoSecure user database into a text file. This provides a thorough and compressible backup of all Cisco Secure ACS internal data.

Using the -l option, you can reload the Cisco Secure ACS internal data from a dump file created by the -d option. For more information about the -l option, see Loading the Cisco Secure ACS Database from a Dump File, page D-11.

**Note** Using the -d option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To dump all Cisco Secure ACS internal data into a text file, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

**Step 2** If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

The CSAuth service stops.

**Step 3** Type:

```
CSUtil.exe -d
```

and press **Enter**.

CSUtil.exe displays a confirmation prompt.

**Step 4** To confirm that you want to dump all Cisco Secure ACS internal data into `dump.txt`, type **Y** and press **Enter**.

CSUtil.exe creates the `dump.txt` file. This process may take a few minutes.



Downloaded from www.Manualslib.com manuals search engine

**Step 5** To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

# Loading the Cisco Secure ACS Database from a Dump File

You can use the -l option to overwrite all Cisco Secure ACS internal data from a dump text file. This option replaces the existing all Cisco Secure ACS internal data with the data in the dump text file. In effect, the -l option initializes all Cisco Secure ACS internal data before loading it from the dump text file. Dump text files are created using the -d option. While the -d option only produces dump text files that are named `dump.txt`, the -l option allows for loading renamed dump files. For more information about creating dump text files, see Creating a Cisco Secure ACS Database Dump File, page D-10.

You can use the -p option in conjunction with the -l option to reset password-aging counters.

**Note** Using the -l option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To load all Cisco Secure ACS internal data from a text file, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

**Step 2** If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

The CSAuth service stops.



Downloaded from www.Manualslib.com manuals search engine

**Step 3** Type:

`CSUtil.exe -l` *filename*

where *filename* is the name of the dump file you want CSUtil.exe to use to load Cisco Secure ACS internal data. Press **Enter**.

CSUtil.exe displays a confirmation prompt for overwriting all Cisco Secure ACS internal data with the data in the dump text file.

**Note** Overwriting the database does not preserve any data; instead, after the overwrite, the database contains only what is specified in the dump text file.

**Step 4** To confirm that you want to replace all Cisco Secure ACS internal data, type **Y** and press **Enter**.

CSUtil.exe initializes all Cisco Secure ACS internal data, and then loads Cisco Secure ACS with the information in the dump file specified. This process may take a few minutes.

**Step 5** To resume user authentication, type:

`net start csauth`

and press **Enter**.

# Compacting the CiscoSecure User Database

Like many relational databases, the CiscoSecure user database handles the deletion of records by marking deleted records as deleted but not removing the records from the database. Over time, your CiscoSecure user database may be substantially larger than is required by the number of users it contains. To reduce the CiscoSecure user database size, you can compact it periodically.



Downloaded from www.Manualslib.com manuals search engine

Compacting the CiscoSecure user database consists of using in conjunction three CSUtil.exe options:

- **-d**—Export all Cisco Secure ACS internal data to a text file named `dump.txt`.
- **-n**—Create a CiscoSecure user database and index.
- **-l**—Load all Cisco Secure ACS internal data from a text file. If you do not specify the filename, CSUtil.exe uses the default file name `dump.txt`.

Additionally, if you want to automate this process, consider using the -q option to suppress the confirmation prompts that otherwise appear before CSUtil.exe performs the -n and -l options.

**Note** Compacting the CiscoSecure user database requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To compact the CiscoSecure user database, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

**Step 2** If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

The CSAuth service stops.

**Step 3** Type:

```
CSUtil.exe -d -n -l
```

Press **Enter**.

**Tip** If you include the -q option in the command, CSUtil.exe does not prompt you for confirmation of initializing or loading the database.



Downloaded from www.Manualslib.com manuals search engine

If you do not use the -q option, CSUtil.exe displays a confirmation prompt for initializing the database and then for loading the database. For more information about the effects of the -n option, see Creating a CiscoSecure User Database, page D-8. For more information about the effects of the -l option, see Loading the Cisco Secure ACS Database from a Dump File, page D-11.

**Step 4** For each confirmation prompt that appears, type **Y** and press **Enter**.

CSUtil.exe dumps all Cisco Secure ACS internal data to `dump.txt`, initializes the CiscoSecure user database, and reloads all Cisco Secure ACS internal data from `dump.txt`. This process may take a few minutes.

**Step 5** To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

# User and AAA Client Import Option

The -i option enables you to update Cisco Secure ACS with data from a colon-delimited text file. You can also update AAA client definitions.

For user accounts, you can add users, change user information such as passwords, or delete users. For AAA client definitions, you can add or delete AAA clients.

This section contains the following topics:


- Importing User and AAA Client Information, page D-15
- User and AAA Client Import File Format, page D-16
  - About User and AAA Client Import File Format, page D-17
  - ONLINE or OFFLINE Statement, page D-17
  - ADD Statements, page D-18
  - UPDATE Statements, page D-19
  - DELETE Statements, page D-21
  - ADD_NAS Statements, page D-21
  - DEL_NAS Statements, page D-23
  - Import File Example, page D-24




Downloaded from www.Manualslib.com manuals search engine

# Importing User and AAA Client Information

To import user or AAA client information, follow these steps:

**Step 1** If you have not performed a backup or dump of Cisco Secure ACS, do so now before proceeding. For more information about backing up the database, see Backing Up Cisco Secure ACS with CSUtil.exe, page D-6.

**Step 2** Create an import text file. For more information about what an import text file can or must contain, see User and AAA Client Import File Format, page D-16.

**Step 3** Copy or move the import text file to the same directory as CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

**Step 4** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe.

**Step 5** Type:

```
CSUtil.exe -i filename
```

where *filename* is the name of the import text file you want CSUtil.exe to use to update Cisco Secure ACS. Press **Enter**.

CSUtil.exe displays a confirmation prompt for updating the database.

**Step 6** To confirm that you want to update Cisco Secure ACS with the information from the import text file specified, type **Y** and press **Enter**.

Cisco Secure ACS is updated with the information in the import text file specified. This process may take a few minutes.

If the import text file contained AAA client configuration data, CSUtil.exe warns you that you need to restart CSTacacs and CSRadius for these changes to take effect.

**Step 7** To restart CSRadius, follow these steps:

**a.** Type:

```
net stop csradius
```

and press **Enter**.

The CSRadius service stops.



Downloaded from www.Manualslib.com manuals search engine

b. To start CSRadius, type:

```
net start csradius
```

and press **Enter**.

**Step 8** To restart CSTacacs, follow these steps:

a. Type:

```
net stop cstacacs
```

and press **Enter**.

The CSTacacs service stops.

b. To start CSTacacs, type:

```
net start cstacacs
```

and press **Enter**.

# User and AAA Client Import File Format

This section contains the following topics:


- About User and AAA Client Import File Format, page D-17
- ONLINE or OFFLINE Statement, page D-17
- ADD Statements, page D-18
- UPDATE Statements, page D-19
- DELETE Statements, page D-21
- ADD_NAS Statements, page D-21
- DEL_NAS Statements, page D-23
- Import File Example, page D-24




Downloaded from www.Manualslib.com manuals search engine

## About User and AAA Client Import File Format

The import file can contain six different line types, as discussed in following topics. The first line of the import file must be one of the tokens defined in Table D-1.

Each line of a CSUtil.exe import file is a series of colon-separated tokens. Some of the tokens are followed by values. Values, like tokens, are colon-delimited. For tokens that require values, CSUtil.exe expects the value of the token to be in the colon-delimited field immediately following the token.

## ONLINE or OFFLINE Statement

CSUtil.exe requires an ONLINE or OFFLINE token in an import text file. The file must begin with a line that contains only an ONLINE or OFFLINE token. The ONLINE and OFFLINE tokens are described in Table D-1.

*Table D-1 ONLINE/OFFLINE Statement Tokens*

| Token | Required | Value Required | Description |
|---|---|---|---|
| ONLINE | Either ONLINE or OFFLINE must be present | — | The CSAuth service remains active while CSUtil.exe imports the text file. CSUtil.exe performance is slower when run in this mode, but Cisco Secure ACS continues to authenticate users during the import. |
| OFFLINE | Either ONLINE or OFFLINE must be present | — | The CSAuth service is stopped while CSUtil.exe imports the text file. Although CSUtil.exe performance is fastest in this mode, no users are authenticated during the import.<br><br>If you need to import a large amount of user information quickly, consider using the OFFLINE token. While performing an import in the OFFLINE mode stops authentication during the import, the import is much faster. For example, importing 100,000 users in the OFFLINE mode takes less than one minute. |



Downloaded from www.Manualslib.com manuals search engine

## ADD Statements

ADD statements are optional. Only the ADD token and its value are required to add a user to Cisco Secure ACS. The valid tokens for ADD statements are listed in Table D-2.

**Note** CSUtil.exe provides no means to specify a particular instance of an external user database type. If a user is to be authenticated by an external user database and Cisco Secure ACS has multiple instances of the specified database type, CSUtil.exe assigns the user to the first instance of that database type. For example, if Cisco Secure ACS has two LDAP external user databases configured, CSUtil.exe creates the user record and assigns the user to the LDAP database that was added to Cisco Secure ACS first.

*Table D-2 ADD Statement Tokens*

| Token | Required | Value Required | Description |
|---|---|---|---|
| ADD | Yes | username | Add user information to Cisco Secure ACS. If the username already exists, no information is changed. |
| PROFILE | No | group number | Group number to which the user is assigned. This must be a number from 0 to 499, not a name. If you do not use the PROFILE token or fail to provide a group number, the user is added to the default group. |
| CHAP | No | CHAP password | Require a CHAP password for authentication. |
| CSDB | No | password | Authenticate the username with the CiscoSecure user database. |
| CSDB_UNIX | No | UNIX-encrypted password | Authenticate the username with the CiscoSecure user database, using a UNIX password format. |
| EXT_NT | No | — | Authenticate the username with a Windows external user database. |
| EXT_NDS | No | — | Authenticate the username with a Novell NDS external user database. |



Downloaded from www.Manualslib.com manuals search engine

*Table D-2 ADD Statement Tokens (continued)*

| Token | Required | Value Required | Description |
|---|---|---|---|
| EXT_SDI | No | — | Authenticate the username with an RSA external user database. |
| EXT_ODBC | No | — | Authenticate the username with an ODBC external user database. |
| EXT_LDAP | No | — | Authenticate the username with a generic LDAP external user database. |
| EXT_LEAP | No | — | Authenticate the username with a LEAP proxy RADIUS server external user database. |
| EXT_RADIUS | No | — | Authenticate the username with a RADIUS token server external user database. |

For example, the following ADD statement would create an account with the username “John”, assign it to Group 3, and specify that John should be authenticated by the CiscoSecure user database with the password “closedmondays”:

```
ADD:John:PROFILE:3:CSDB:closedmondays
```

## UPDATE Statements

UPDATE statements are optional. They make changes to existing user accounts. Only the UPDATE token and its value are required by CSUtil.exe, but if no other tokens are included, no changes are made to the user account. You can use the UPDATE statement to update the group a user is assigned to or to update which database Cisco Secure ACS uses to authenticate the user. The valid tokens for UPDATE statements are listed in Table D-3.



Downloaded from www.Manualslib.com manuals search engine

*Table D-3 UPDATE Statement Tokens*

| Token | Required | Value Required | Description |
|---|---|---|---|
| UPDATE | Yes | username | Update user information to Cisco Secure ACS. |
| PROFILE | No | group number | Group number to which the user is assigned. This must be a number from 0 to 499, not a name.<br>**Note** If you do not specify a database token, such as CSDB or EXT_NT, updating a group assignment may erase a user's password. |
| CHAP | No | CHAP password | Require a CHAP password for authentication. |
| CSDB | No | password | Authenticate the username with the CiscoSecure user database. |
| CSDB_UNIX | No | UNIX-encrypted password | Authenticate the username with the CiscoSecure user database, using a UNIX password format. |
| EXT_NT | No | — | Authenticate the username with a Windows external user database. |
| EXT_NDS | No | — | Authenticate the username with a Novell NDS external user database. |
| EXT_ODBC | No | — | Authenticate the username with an ODBC external user database. |
| EXT_LDAP | No | — | Authenticate the username with a generic LDAP external user database. |
| EXT_LEAP | No | — | Authenticate the username with a LEAP proxy RADIUS server external user database. |
| EXT_RADIUS | No | — | Authenticate the username with a RADIUS token server external user database. |



Downloaded from www.Manualslib.com manuals search engine

For example, the following UPDATE statement causes CSUtil.exe to update the account with username "John", assign it to Group 50, specify that John should be authenticated by a UNIX-encrypted password, with a separate CHAP password "goodoldchap":

```
UPDATE:John:PROFILE:50:CSDB_UNIX:3Al3qf9:CHAP:goodoldchap
```

## DELETE Statements

DELETE statements are optional. The DELETE token and its value are required to delete a user account from Cisco Secure ACS. The DELETE token, detailed in Table D-4, is the only token in a DELETE statement.

***Table D-4 UPDATE Statement Tokens***

| Token | Required | Value Required | Description |
|---|---|---|---|
| DELETE | Yes | username | The name of the user account that is to be deleted. |

For example, the following DELETE statement causes CSUtil.exe to permanently remove the account with username "John" from the CiscoSecure user database:

```
DELETE:John
```

## ADD_NAS Statements

ADD_NAS statements are optional. The ADD_NAS, IP, KEY, and VENDOR tokens and their values are required to add a AAA client definition to Cisco Secure ACS. The valid tokens for ADD_NAS statements are listed in Table D-5.



Downloaded from www.Manualslib.com manuals search engine

*Table D-5 ADD_NAS Statement Tokens*

| Token | Required | Value Required | Description |
|---|---|---|---|
| ADD_NAS | Yes | AAA client name | The name of the AAA client that is to be added. |
| IP | Yes | IP address | The IP address of the AAA client being added. |
| KEY | Yes | Shared secret | The shared secret for the AAA client. |
| VENDOR | Yes | See description | The authentication protocol the AAA client uses. For RADIUS, this includes the VSA.<br>**Note** The valid values are listed below. Quotation marks are required due to the spaces in the protocol names.<br>• "TACACS+ (Cisco IOS)"<br>• "RADIUS (Cisco Aironet)"<br>• "RADIUS (Cisco BBSM)"<br>• "RADIUS (Cisco IOS/PIX)"<br>• "RADIUS (Cisco VPN 3000)"<br>• "RADIUS (Cisco VPN 5000)"<br>• "RADIUS (IETF)"<br>• "RADIUS (Ascend)"<br>• "RADIUS (Juniper)"<br>• "RADIUS (Nortel)"<br>• "RADIUS (iPass)" |
| NDG | No | NDG name | The name of the Network Device Group to which the AAA client is to be added. |



Downloaded from www.Manualslib.com manuals search engine

*Table D-5 ADD_NAS Statement Tokens (continued)*

| Token | Required | Value Required | Description |
|---|---|---|---|
| SINGLE_CON | No | Y or N | For AAA clients using TACACS+ only, the value set for this TOKEN specifies whether the Single Connect TACACS+ AAA Client option is enabled. For more information, see Adding a AAA Client, page 4-16. |
| KEEPALIVE | No | Y or N | For AAA clients using TACACS+ only, the value set for this token specifies whether the Log Update/Watchdog Packets from this Access Server option is enabled. For more information, see Adding a AAA Client, page 4-16. |

For example, the following ADD_NAS statement causes CSUtil.exe to add a AAA client with the name "SVR2-T+", using TACACS+ with the single connection and keep alive packet options enabled:

ADD_NAS:SVR2-T+:IP:*IP address*:KEY:*shared secret*:VENDOR:"TACACS+ (Cisco IOS)":NDG:"East Coast":SINGLE_CON:Y:KEEPALIVE:Y

## DEL_NAS Statements

DEL_NAS statements are optional. The DEL_NAS token, detailed in Table D-6, is the only token in a DEL_NAS statement. DEL_NAS statements delete AAA client definitions from Cisco Secure ACS.

*Table D-6 DEL_NAS Statement Tokens*

| Token | Required | Value Required | Description |
|---|---|---|---|
| DEL_NAS | Yes | AAA client name | The name of the AAA client that is to be deleted. |

For example, the following DEL_NAS statement causes CSUtil.exe to delete a AAA client with the name "SVR2-T+":

```
DEL_NAS:SVR2-T+
```



Downloaded from www.Manualslib.com manuals search engine

## Import File Example

The following is an example import text file:

```
OFFLINE
ADD:user01:CSDB:userpassword:PROFILE:1
ADD:user02:EXT_NT:PROFILE:2
ADD:chapuser:CSDB:hello:CHAP:chappw:PROFILE:3
ADD:mary:EXT_NT:CHAP:achappassword
ADD:joe:EXT_SDI
ADD:vanessa:CSDB:vanessaspassword
ADD:juan:CSDB_UNIX:unixpassword
UPDATE:foobar:PROFILE:10
DELETE:paul
ADD_NAS:SVR2-T+:IP:209.165.202.136:KEY:A87il032bzg:VENDOR:"TACACS+ (Cisco IOS)":NDG:"East
Coast"
DEL_NAS:SVR16-RAD
```

# Exporting User List to a Text File

You can use the -u option to export a list of all users in the CiscoSecure user database to a text file named `users.txt`. The `users.txt` file organizes users by group. Within each group, users are listed in the order that their user accounts were created in the CiscoSecure user database. For example, if accounts were created for Pat, Dana, and Lloyd, in that order, `users.txt` lists them in that order as well, rather than alphabetically.

**Note** Using the -u option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To export user information from the CiscoSecure user database into a text file, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

The CSAuth service stops.

**Step 3** Type:

```
CSUtil.exe -u
```

and press **Enter**.

CSUtil.exe exports information for all users in the CiscoSecure user database to a file named `users.txt`.

**Step 4** To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

# Exporting Group Information to a Text File

You can use the -g option to export group configuration data, including device command sets, from the CiscoSecure user database to a text file named `groups.txt`. The `groups.txt` file is useful primarily for debugging purposes while working with the TAC.

**Note** Using the -g option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To export group information from the CiscoSecure user database to a text file, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** If the CSAuth service is running, type:

```
net stop csauth
```

and press **Enter**.

The CSAuth service stops.

**Step 3** Type:

```
CSUtil.exe -g
```

and press **Enter**.

CSUtil.exe exports information for all groups in the CiscoSecure user database to a file named `groups.txt`.

**Step 4** To resume user authentication, type:

```
net start csauth
```

and press **Enter**.

# Exporting Registry Information to a Text File

You can use the -y option to export Windows Registry information for Cisco Secure ACS. CSUtil.exe exports the Registry information to a file named `setup.txt`. The `setup.txt` file is primarily useful for debugging purposes while working with the TAC.

To export Registry information from Cisco Secure ACS to a text file, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

**Step 2** Type:

```
CSUtil.exe -y
```

and press **Enter**.



Downloaded from www.Manualslib.com manuals search engine

CSUtil.exe exports Windows Registry information for Cisco Secure ACS to a file named `setup.txt`.

# Decoding Error Numbers

You can use the -e option to decode error numbers found in Cisco Secure ACS service logs. These are error codes internal to Cisco Secure ACS. For example, the CSRadius log could contain a message similar to the following:

```
CSRadius/Logs/RDS.log:RDS 05/22/2001 10:09:02 E 2152 4756 Error -1087 authenticating geddy
- no NAS response sent
```

In this example, the error code number that you could use CSUtil.exe to decode is "-1087":

```
C:\Program Files\CiscoSecure ACS vx.x\Utils: CSUtil.exe -e -1087
CSUtil v3.0(1.14), Copyright 1997-2001, Cisco Systems Inc
Code -1087 : External database reported error during authentication
```

**Note** The -e option applies to Cisco Secure ACS internal error codes only, not to Windows error codes sometimes captured in Cisco Secure ACS logs, such as when Windows authentication fails.

For more information about Cisco Secure ACS service logs, see Service Logs, page 11-31.

To decode an error number from a Cisco Secure ACS service log, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Type:

`CSUtil.exe -e -`*number*

where *number* is the error number found in the Cisco Secure ACS service log. Press **Enter**.

**Note** The hyphen (-) before *number* is required.

CSUtil.exe displays the text message equivalent to the error number specified.

# Recalculating CRC Values

The -c option is for use by the TAC. Its purpose is to resolve CRC (cyclical redundancy check) value conflicts between files manually copied into your Cisco Secure ACS directories and the values recorded in the Windows Registry.

**Note** Do not use the -c option unless a Cisco representative requests that you do.

# User-Defined RADIUS Vendors and VSA Sets

This section provides information and procedures about user-defined RADIUS vendors and VSAs.

This section contains the following topics:


- About User-Defined RADIUS Vendors and VSA Sets, page D-29
- Adding a Custom RADIUS Vendor and VSA Set, page D-29
- Deleting a Custom RADIUS Vendor and VSA Set, page D-31
- Listing Custom RADIUS Vendors, page D-32
- Exporting Custom RADIUS Vendor and VSA Sets, page D-33
- RADIUS Vendor/VSA Import File, page D-34




Downloaded from www.Manualslib.com manuals search engine

# About User-Defined RADIUS Vendors and VSA Sets

In addition to supporting a set of predefined RADIUS vendors and vendor-specific attributes (VSAs), Cisco Secure ACS supports RADIUS vendors and VSAs that you define. We recommend that you use RDBMS Synchronization to add and configure custom RADIUS vendors; however, you can use CSUtil.exe to accomplish the same custom RADIUS vendor and VSA configurations that you can accomplish using RDBMS Synchronization. Custom RADIUS vendor and VSA configuration created by either of these two features—RDBMS Synchronization or CSUtil.exe—can be modified by the other feature. Choosing one feature for configuring custom RADIUS vendors and VSAs does not preclude using the other feature. For more information about RDMBS Synchronization, see RDBMS Synchronization, page 9-25.

Vendors you add must be IETF-compliant; therefore, all VSAs that you add must be sub-attributes of IETF RADIUS attribute number 26. You can define up to ten custom RADIUS vendors, numbered 0 (zero) through 9. CSUtil.exe allows only one instance of any given vendor, as defined by the unique vendor IETF ID number and by the vendor name.

**Note** If you intend to replicate user-defined RADIUS vendor and VSA configurations, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary Cisco Secure ACSes, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy. For more information about database replication, see CiscoSecure Database Replication, page 9-1.

# Adding a Custom RADIUS Vendor and VSA Set

You can use the -addUDV option to add up to ten custom RADIUS vendors and VSA sets to Cisco Secure ACS. Each RADIUS vendor and VSA set is added to one of ten possible user-defined RADIUS vendor slots.

**Note** While CSUtil.exe adds a custom RADIUS vendor and VSA set to Cisco Secure ACS, all Cisco Secure ACS services are automatically stopped and restarted. No users are authenticated during this process.



Downloaded from www.Manualslib.com manuals search engine

### Before You Begin

- Define a custom RADIUS vendor and VSA set in a RADIUS vendor/VSA import file. For more information, see RADIUS Vendor/VSA Import File, page D-34.
- Determine the RADIUS vendor slot to which you want to add the new RADIUS vendor and VSAs. For more information, see Listing Custom RADIUS Vendors, page D-32.
- Make sure that regedit is not running. If regedit is running on the Cisco Secure ACS Windows server, it can prevent Registry updates required for adding a custom RADIUS vendor and VSA set.

To add a custom RADIUS VSA to Cisco Secure ACS, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

**Step 2** Type:

`CSUtil.exe -addUDV` *slot-number filename*

where *slot-number* is an unused Cisco Secure ACS RADIUS vendor slot and *filename* is the name of a RADIUS vendor/VSA import file. The *filename* can include a relative or absolute path to the RADIUS vendor/VSA import file. Press **Enter**.

For example, to add the RADIUS vendor defined in `d:\acs\myvsa.ini` to slot 5, the command would be:

```
CSUtil.exe -addUDV 5 d:\acs\myvsa.ini
```

CSUtil.exe displays a confirmation prompt.

**Step 3** To confirm that you want to add the RADIUS vendor and halt all Cisco Secure ACS services during the process, type **Y** and press **Enter**.

CSUtil.exe halts Cisco Secure ACS services, parses the vendor/VSA input file, and adds the new RADIUS vendor and VSAs to Cisco Secure ACS. This process may take a few minutes. After it is complete, CSUtil.exe restarts Cisco Secure ACS services.



Downloaded from www.Manualslib.com manuals search engine

**Note** We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the Utils directory, where CSUtil.exe is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

# Deleting a Custom RADIUS Vendor and VSA Set

You can use the -delUDV option to delete a custom RADIUS vendor from Cisco Secure ACS.

**Note** While CSUtil.exe deletes a custom RADIUS vendor from Cisco Secure ACS, all Cisco Secure ACS services are automatically stopped and restarted. No users are authenticated while this process is occurring.

### Before You Begin

Verify that, in the Network Configuration section of the Cisco Secure ACS HTML interface, no AAA client uses the RADIUS vendor. For more information about configuring AAA clients, see AAA Client Configuration, page 4-11.

Verify that your RADIUS accounting log does not contain attributes from the RADIUS vendor you want to delete. For more information about configuring your RADIUS accounting log, see Accounting Logs, page 11-6.

To delete a custom RADIUS vendor and VSA set from Cisco Secure ACS, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Type:

`CSUtil.exe -delUDV` *slot-number*

where *slot-number* is the slot containing the RADIUS vendor that you want to delete. Press **Enter**.

**Note** For more information about determining what RADIUS vendor a particular slot contains, see Listing Custom RADIUS Vendors, page D-32.

CSUtil.exe displays a confirmation prompt.

**Step 3** To confirm that you want to halt all Cisco Secure ACS services while deleting the custom RADIUS vendor and VSAs, type **Y** and press **Enter**.

CSUtil.exe displays a second confirmation prompt.

**Step 4** To confirm that you want to delete the RADIUS vendor, type **Y** and press **Enter**.

CSUtil.exe halts Cisco Secure ACS services, deletes the specified RADIUS vendor from Cisco Secure ACS. This process may take a few minutes. After it is complete, CSUtil.exe restarts Cisco Secure ACS services.

# Listing Custom RADIUS Vendors

You can use the -listUDV option to determine what custom RADIUS vendors are defined in Cisco Secure ACS. This option also enables you to determine which of the ten possible custom RADIUS vendor slots are in use and which RADIUS vendor occupies each used slot.

To list all custom RADIUS vendors defined in Cisco Secure ACS, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Type:

```
CSUtil.exe -listUDV
```

Press **Enter**.

CSUtil.exe lists each user-defined RADIUS vendor slot in slot number order. CSUtil.exe lists slots that do not contain a custom RADIUS vendor as "Unassigned". An unassigned slot is empty. You can add a custom RADIUS vendor to any slot listed as "Unassigned".

# Exporting Custom RADIUS Vendor and VSA Sets

You can export all custom RADIUS vendor and VSA sets to files. Each vendor and VSA set is saved to a separate file. The files created by this option are in the same format as RADIUS vendor/VSA import files. This option is particularly useful if you need to modify a custom RADIUS vendor and VSA set and you have misplaced the original file used to import the set.

**Note** Exporting a custom RADIUS vendor and VSA set does not remove the vendor and VSA set from Cisco Secure ACS.

Cisco Secure ACS places all exported vendor/VSA files in a subdirectory of the directory containing CSUtil.exe. The subdirectory is named `System UDVs`. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.

Each exported vendor/VSA file is named `UDV_`*n*`.ini`, where *n* is the slot number currently occupied by the custom RADIUS vendor and VSA set. For example, if vendor Widget occupies slot 4, the exported file created by CSUtil.exe is `UDV_4.ini`.

To export custom RADIUS vendor and VSA sets to files, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe. For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files, page D-2.



Downloaded from www.Manualslib.com manuals search engine

**Step 2** Type:

```
CSUtil.exe -dumpUDV
```

Press **Enter**.

For each custom RADIUS vendor and VSA set currently configured in Cisco Secure ACS, CSUtil.exe writes a file in the `System UDVs` subdirectory.

# RADIUS Vendor/VSA Import File

To import a custom RADIUS vendor and VSA set into Cisco Secure ACS, you must define the RADIUS vendor and VSA set in an import file. This section details the format and content of RADIUS VSA import files.

We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the `Utils` directory, where CSUtil.exe is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

This section contains the following topics:


- About the RADIUS Vendor/VSA Import File, page D-34
- Vendor and VSA Set Definition, page D-35
- Attribute Definition, page D-36
- Enumeration Definition, page D-38
- Example RADIUS Vendor/VSA Import File, page D-39


## About the RADIUS Vendor/VSA Import File

RADIUS Vendor/VSA import files use a Windows .ini file format. Each RADIUS vendor/VSA import file comprises three types of sections, detailed in Table D-7. Each section comprises a section header and a set of keys and values. The order of the sections in the RADIUS vendor/VSA import file is irrelevant.



Downloaded from www.Manualslib.com manuals search engine

*Table D-7 RADIUS VSA Import File Section Types*

| Section | Required | Number | Description |
|---|---|---|---|
| Vendor and VSA set definition | Yes | 1 | Defines the RADIUS vendor and VSA set. For more information, see Vendor and VSA Set Definition, page D-35. |
| Attribute definition | Yes | 1 to 255 | Defines a single attribute of the VSA set. For more information, see Attribute Definition, page D-36. |
| Enumeration | No | 0 to 255 | Defines enumerations for attributes with integer data types. For more information, see Enumeration Definition, page D-38. |

## Vendor and VSA Set Definition

Each RADIUS vendor/VSA import file must have one vendor and VSA set section. The section header must be "[User Defined Vendor]". Table D-8 lists valid keys for the vendor and VSA set section.

*Table D-8 Vendor and VSA Set Keys*

| Keys | Required | Value Required | Description |
|---|---|---|---|
| Name | Yes | Vendor name | The name of the RADIUS vendor. |
| IETF Code | Yes | An integer | The IETF-assigned vendor number for this vendor. |
| VSA *n* (where *n* is the VSA number) | Yes—you can define 1 to 255 VSAs | Attribute name | The name of a VSA. For each VSA named here, the file must contain a corresponding attribute definition section.<br>**Note** Attribute names must be unique within the RADIUS vendor/VSA import file, and within the set of all RADIUS attributes in Cisco Secure ACS. To facilitate this, we recommend that you prefix the vendor name to each attribute name, such as "widget-encryption" for an encryption-related attribute for the vendor Widget. This also makes accounting logs easier to understand. |



Downloaded from www.Manualslib.com manuals search engine

For example, the following vendor and VSA set section defines the vendor "Widget", whose IETF-assigned vendor number is 9999. Vendor Widget has 4 VSAs (thus requiring 4 attribute definition sections):

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
```

## Attribute Definition

Each RADIUS vendor/VSA import file must have one attribute definition section for each attribute defined in the vendor and VSA set section. The section header of each attribute definition section must match the attribute name defined for that attribute in the vendor and VSA set section. Table D-8 lists the valid keys for an attribute definition section.



Downloaded from www.Manualslib.com manuals search engine

*Table D-9 Attribute Definition Keys*

| Keys | Required | Value Required | Description |
|---|---|---|---|
| Type | Yes | See Description | The data type of the attribute. It must be one of the following:<br>• STRING<br>• INTEGER<br>• IPADDR<br>If the attribute is an integer, the Enums key is valid. |
| Profile | Yes | See Description | The attribute profile defines if the attribute is used for authorization or accounting (or both). At least one of the following two values must be present in the Profile key definition:<br>• **IN**—The attribute is used for accounting. After you add the attribute to Cisco Secure ACS, you can configure your RADIUS accounting log to record the new attribute. For more information about RADIUS accounting logs, see Accounting Logs, page 11-6.<br>• **OUT**—The attribute is used for authorization.<br>In addition, you can use the value "MULTI" to allow several instances of the attribute per RADIUS message.<br>Combinations are valid. For example:<br>`Profile=MULTI OUT`<br>or<br>`Profile=IN OUT` |
| Enums | No (only valid when the TYPE value is INTEGER) | Enumera-tions section name | The name of the enumeration section.<br>**Note** Several attributes can reference the same enumeration section. For more information, see Enumeration Definition, page D-38. |



Downloaded from www.Manualslib.com manuals search engine

For example, the following attribute definition section defines the widget-encryption VSA, which is an integer used for authorization, and for which enumerations exist in the Encryption-Types enumeration section:

```
[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types
```

## Enumeration Definition

Enumeration definitions enable you to associate a text-based name for each valid numeric value of an integer-type attribute. In the Group Setup and User Setup sections of the Cisco Secure ACS HTML interface, the text values you define appear in lists associated with the attributes that use the enumerations. Enumeration definition sections are required only if an attribute definition section references them. Only attributes that are integer-type attributes can reference an enumeration definition section.

The section header of each enumeration definition section must match the value of an Enums key that references it. An enumeration definition section can be referenced by more than one Enums key, thus allowing for reuse of common enumeration definitions. An enumeration definition section can have up to 1000 keys.

Table D-10 lists the valid keys for an enumeration definition section.



Downloaded from www.Manualslib.com manuals search engine

*Table D-10 Enumerations Definition Keys*

| Keys | Required | Value Required | Description |
|---|---|---|---|
| *n*<br>(See description.) | Yes | String | For each valid integer value of the corresponding attribute, an enumerations section must have one key.<br>Each key defines a string value associated with an integer value. Cisco Secure ACS uses these string values in the HTML interface.<br>For example, if 0 through 4 are valid integer values for a given attribute, its enumeration definition would contain the following:<br>`0=`*value0*<br>`1=`*value1*<br>`2=`*value2*<br>`3=`*value3*<br>`4=`*value4* |

For example, the following enumerations definition section defines the Encryption-Types enumeration, which associates the string value 56-bit with the integer 0 and the string value 128-bit with the integer 1:

```
[Encryption-Types]
0=56-bit
1=128-bit
```

## Example RADIUS Vendor/VSA Import File

The example RADIUS vendor/VSA import file, below, defines the vendor Widget, whose IETF number is 9999. The vendor Widget has 5 VSAs. Of those attributes, 4 are for authorization and one is for accounting. Only one attribute can have multiple instances in a single RADIUS message. Two attributes have enumerations for their valid integer values and they share the same enumeration definition section.

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
```



Downloaded from www.Manualslib.com manuals search engine

```
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
VSA 5=widget-remote-address

[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-admin-interface]
Type=IPADDR
Profile=OUT

[widget-group]
Type=STRING
Profile=MULTI OUT

[widget-admin-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-remote-address]
Type=STRING
Profile=IN

[Encryption-Types]
0=56-bit
1=128-bit
2=256-bit
```

# PAC File Generation

You can use the -t option to generate PAC files for use with EAP-FAST clients. For more information about PACs and EAP-FAST, see EAP-FAST Authentication, page 10-13.

This section contains the following topics:


- PAC File Options and Examples, page D-41
- Generating PAC Files, page D-43




Downloaded from www.Manualslib.com manuals search engine

# PAC File Options and Examples

When you use the -t option generate PAC files with CSUtil.exe, you have the following additional options.

- **User specification options**—While you can choose which user specification option you want to use, you **must** choose one of the four options for specifying which users you want PAC files for; otherwise, CSUtil.exe displays an error message because no users are specified. User specification options are as follows:
  - **-a**—CSUtil.exe generates a PAC file for each user in the CiscoSecure user database. For example, if you have 3278 users in the CiscoSecure user database and ran **CSUtil.exe -t -a**, CSUtil.exe would generate 3278 PAC files, one for each user.

**Note** Using the -a option restarts the CSAuth service. No users are authenticated while CSAuth is unavailable.

  - **-g** *N*—CSUtil.exe generates a PAC file for each user in the user group specified by number (*N*). Cisco Secure ACS has 500 groups, numbered from 0 (zero) to 499. For example, if group 7 has 43 users and you ran **CSUtil.exe -t -g 7**, CSUtil.exe would generate 43 PAC files, one for each user who is a member of group 7.

**Note** Using the -g option restarts the CSAuth service. No users are authenticated while CSAuth is unavailable.

  - **-u** *username*—CSUtil.exe generates a PAC file for the user specified by name (*username*). For example, if you ran **CSUtil.exe -t -u seaniemop**, CSUtil.exe would generate a single PAC file, named `seaniemop.pac`.

**Tip** You can also specify a domain-qualified username, using the format *DOMAIN\username*. For example, if you specify `ENIGINEERING\augustin`, Cisco Secure ACS generates a PAC file name `ENGINEERING_augustin.pac`.



Downloaded from www.Manualslib.com manuals search engine

– **-f** *list*—CSUtil.exe generates a PAC file for each username contained in the file specified, where *list* represents the full path and filename of the list of usernames.

  Lists of usernames should contain one username per line with no additional spaces or other characters.

  For example, if list.txt in d:\temp\pacs contains the following usernames:

```
seaniemop
jwiedman
echamberlain
```

  and you ran **CSUtil.exe -t -f d:\temp\pacs\list.txt**, CSUtil.exe generates three PAC files: `seaniemop.pac`, `jwiedman.pac`, and `echamberlain.pac`.

**Tip** You can also specify domain-qualified usernames, using the format *DOMAIN\username*. For example, if you specify `ENIGINEERING\augustin`, Cisco Secure ACS generates a PAC file name `ENGINEERING_augustin.pac`.

- **-passwd** *password*—CSUtil.exe uses the password specified, rather than the default password, to protect the PAC files it generates. The password you specify is required when the PACs it protects are loaded into an EAP-FAST end-user client.

  **Note** We recommend that you use a password you devise rather than the default password.

  PAC passwords can contain any character, are between four and 128 characters long, and case sensitive. While CSUtil.exe does not enforce strong password rules, we recommend that you use a strong password, that is, your PAC password should:

  – Be very long.
  – Contain uppercase and lowercase letters.
  – Contain numbers in addition to letters.
  – Contain no common words or names.



Downloaded from www.Manualslib.com manuals search engine

# Generating PAC Files

**Note** If you use the -a or -g option during PAC file generation, CSUtil.exe restarts the CSAuth service. No users are authenticated while CSAuth is unavailable.

For more information about PACs, see About PACs, page 10-17.

To generate PAC files, follow these steps:

**Step 1** Use the discussion in PAC File Options and Examples, page D-41, to determine the following:

- Which users you want to generate PAC files for. If you want to use a list of users, create it now.
- What password you want to use to protect the PAC files you generate. If necessary, create a password. We recommend passwords that are long, use uppercase and lowercase letters, and include numbers.
- The full path to the directory you want the PAC files to be created in. If necessary, create the directory.

**Step 2** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe.

**Step 3** Type

`CSUtil.exe -t` *additional arguments*

where *additional arguments* represents at least one option for specifying which users to generate PAC files for. You can also use the options to specify filepath and password.

Press **Enter**.

CSUtil.exe generates the PAC files for each user specified. The PAC files are named with the username plus a ".pac" file extension. For example, a PAC file for the username `seaniemop` would be `seaniemop.pac` and a PAC file for the domain-qualified username `ENGINEERING\augustin` would be `ENGINEERING_augustin.pac`.



Downloaded from www.Manualslib.com manuals search engine

If you specified a filepath, the PAC files are saved where you specified. You can distribute the PAC files to the applicable end-user clients.

# Posture Validation Attributes

You can use CSUtil.exe to export, add, and delete posture validation attributes, which are essential to Network Admission Control (NAC). For more information about NAC, see Chapter 14, "Network Admission Control".

This section contains the following topics:


- Posture Validation Attribute Definition File, page D-44
- Exporting Posture Validation Attribute Definitions, page D-48
- Importing Posture Validation Attribute Definitions, page D-49
- Deleting a Posture Validation Attribute Definition, page D-51
- Default Posture Validation Attribute Definition File, page D-52


## Posture Validation Attribute Definition File

A posture validation attribute definition file is a text file that contains one or more posture validation attribute definitions. Each definition consists of a definition header and several values, described below. For an example of the contents of a posture validation attribute definition file, see Default Posture Validation Attribute Definition File, page D-52.

With the exception of the attribute definition header, each attribute definition value must be formatted as follows:

*name=value*

where *name* is the value name and *value* is a string or integer, as specified in the list below.

**Tip** Use a semi-colon to identify lines that are comments.



Downloaded from www.Manualslib.com manuals search engine

Example D-1 shows an example of a posture validation attribute definition, including a comment after the attribute definition:

### *Example D-1 Example Attribute Definition*

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

; attribute 1 is reserved for the APT
```

A posture validation attribute is uniquely defined by the combination of its vendor ID, application ID, and attribute ID. The following list provides details of these values and of each line required in an attribute definition:

- **[attr#*n*]**—Attribute definition header, where *n* is a unique, sequential integer, beginning with zero. CSUtil.exe uses the definition header to distinguish the beginning of a new attribute definition. Each attribute definition *must* begin with a line containing the definition header. The first attribute definition in the file *must* have the header `[attr#0]`, the second attribute definition in a file must have the header `[attr#1]`, and so on. A break in the numbering causes CSUtil.exe to ignore attribute definitions at the break and beyond. For example, if a file with 10 attribute definitions the fifth attribute is defined as `[attr#5]` instead of `[attr#4]`, CSUtil.exe ignores the attribute defined as `[attr#5]` and remaining five the attributes following it.

**Tip** The value of *n* is irrelevant to any of the ID values in the attribute definition file. For example, the 28th definition in a file must have the header `[attr#27]`, but this does not limit or otherwise define valid values for vendor-id, application-id, attribute-id. Neither does it limit or define the number of posture validation attributes supported by Cisco Secure ACS.

- **vendor-id**—An unsigned integer, the vendor number is of the vendor associated with the posture validation attribute. The vendor number should be the number assigned to the vendor in the IANA Assigned Numbers RFC. For example, vendor ID 9 corresponds to Cisco Systems, Inc.



Downloaded from www.Manualslib.com manuals search engine

Vendor IDs have one or more applications associated with them, identified by the application-id value.

- **vendor-name**—A string, the vendor name appears in the Cisco Secure ACS HTML interface and logs for the associated posture validation attribute. For example, any attribute definition with a vendor ID of 9 could have a vendor name “Cisco”.

**Note** The vendor name cannot differ for each attribute that shares the same vendor ID. For example, you cannot add an attribute with a vendor-id of 9 if the vendor-name is not “Cisco”.

- **application-id**—An unsigned integer, the application ID uniquely identifies the vendor application associated with the posture validation attribute. For example, if the vendor ID is 9 and the application ID is 1, the posture validation attribute is associated with the Cisco application with an ID of 1, which is the Cisco Trust Agent (CTA), also known as a posture agent (PA).
- **application-name**—A string, the application name appears in the Cisco Secure ACS HTML interface and logs for the associated posture validation attribute. For example, if the vendor ID is 9 and the application ID is 1, the application name would be “PA”, an abbreviation of posture agent, which is another term for CTA.

**Note** The application name cannot differ for each attribute that shares the same vendor ID and application ID pair. For example, you cannot add an attribute with a vendor-id of 9 and application ID of 1 if the application-name is not “PA”.

- **attribute-id**—An unsigned integer in the range of 1 to 65535, the attribute ID uniquely identifies the posture validation attribute for the vendor ID and application ID specified.

**Note** For each application, attributes 1 and 2 are reserved. If you add attributes that imply a new application, CSUtil.exe automatically creates attribute 1 as Application-Posture-Token and attribute 2 as System-Posture-Token.



Downloaded from www.Manualslib.com manuals search engine

- **attribute-name**—A string, the attribute name appears in the Cisco Secure ACS HTML interface and logs for the associated posture validation attribute. For example, if the vendor ID is 9, the application ID is 1, and the attribute ID is 1, the attribute name is "Application-Posture-Token".
- **attribute-profile**—A string, the attribute profile specifies whether Cisco Secure ACS can send the attribute in a posture validation response, can receive the attribute in a posture validation request, or can both send and receive the attribute during posture validation. Valid values for attribute-profile are:
  - **in**—Cisco Secure ACS accepts the attribute in posture validation requests and can log the attribute, and you can use it in local policy rule definitions. Attributes with an "in" attribute-profile are also known as inbound attributes.
  - **out**—Cisco Secure ACS can send the attribute in posture validation responses but you cannot use it in local policy rule definitions. Attributes with an "out" attribute-profile are also known as outbound attributes. The only outbound attributes that you can configure Cisco Secure ACS to log are the attributes for Application Posture Tokens and System Posture Tokens; however, these are system-defined attributes that you cannot modify.
  - **in out**—Cisco Secure ACS both accepts the attribute in posture validation requests and can send the attribute in posture validation responses. Attributes with an "in out" attribute-profile are also known as both inbound and outbound attributes.
- **attribute-type**—A string, the attribute type specifies the kind of data that is valid in the associated attribute. For attributes whose attribute-profile is `in` or `in out`, the attribute-type determines the types of operators available for defining local policy rules that use the attribute. An example of an inbound attribute is the ServicePacks attribute sent by CTA. An example of an outbound attribute is the System-Posture-Token attribute, sent to CTA.

  Valid values of attribute-type are:
  - boolean
  - string
  - integer
  - unsigned integer
  - ipaddr



Downloaded from www.Manualslib.com manuals search engine

- date
- version
- octet-array

For more information about attribute data types, see NAC Attribute Data Types, page 14-19.

# Exporting Posture Validation Attribute Definitions

The -dumpAVP option exports the current posture validation attributes to an attribute definition file. For an explanation of the contents of a posture validation attribute definition file, see Posture Validation Attribute Definition File, page D-44. For an example of an attribute definition file, see Default Posture Validation Attribute Definition File, page D-52.

To export posture validation attributes, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe.

**Step 2** Type:

`CSUtil.exe -dumpavp` *filename*

where *filename* is the name of the file in which you want CSUtil.exe to write all attribute definitions. Press **Enter**.

**Tip** When you specify *filename*, you can prefix the filename with a relative or absolute path, too. For example, `CSUtil.exe -dumpavp c:\temp\allavp.txt` writes the file allavp.txt in c:\temp.

**Step 3** If you are prompted to confirm overwriting a file with the same path and name that you specified in Step 2, do one of the following:

- To overwrite the file, type **Y** and press **Enter**.

**Tip** To force CSUtil.exe to overwrite an existing file, use the -q option: **CSUtil.exe -q -dumpavp** *filename*.



Downloaded from www.Manualslib.com manuals search engine

- To preserve the file, type **N**, press **Enter**, and return to Step 2.

CSUtil.exe writes all posture validation attribute definitions in the file specified. To view the contents of the file, use the text editor of your choice.

# Importing Posture Validation Attribute Definitions

The -addAVP option imports into Cisco Secure ACS posture validation attribute definitions from an attribute definition file. For an explanation of the contents of a posture validation attribute definition file, see Posture Validation Attribute Definition File, page D-44. For an example of an attribute definition file, see Default Posture Validation Attribute Definition File, page D-52.

**Before You Begin**

Because completing this procedure requires restarting the CSAuth service, which temporarily suspends authentication services, consider performing this procedure when demand for Cisco Secure ACS services is low.

Use the steps in Exporting Posture Validation Attribute Definitions, page D-48, to create a backup of posture validation attribute definitions. You can also use the exported attribute definition file to double-check the vendor ID, application ID, and attribute ID of current posture validation attributes.

To import posture validation attributes, follow these steps:

**Step 1** Use the discussion in Posture Validation Attribute Definition File, page D-44, to create a properly formatted attribute definition file. Place the file either in the directory containing CSUtil.exe or a directory accessible from the computer running Cisco Secure ACS.

**Step 2** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe.

**Step 3** Type:

`CSUtil.exe -addavp` *filename*

where *filename* is the name of the file in which you want CSUtil.exe to write all attribute definitions. Press **Enter**.



Downloaded from www.Manualslib.com manuals search engine

**Tip** When you specify *filename*, you can prefix the filename with a relative or absolute path, too. For example, `CSUtil.exe -addavp c:\temp\addavp.txt` writes the file addavp.txt in c:\temp.

CSUtil.exe adds or modifies the attributes specified in the file. An example of a successful addition of nine posture validation attributes follows:

```
C:.../Utils 21: csutil -addavp myavp.txt
CSUtil v3.3(1.6), Copyright 1997-2001, Cisco Systems Inc
Attribute 9876:1:11 (Calliope) added to registry
Attribute 9876:1:3 (Clio) added to registry
Attribute 9876:1:4 (Erato) added to registry
Attribute 9876:1:5 (Euterpe) added to registry
Attribute 9876:1:6 (Melpomene) added to registry
Attribute 9876:1:7 (Polyhymnia) added to registry
Attribute 9876:1:8 (Terpsichore) added to registry
Attribute 9876:1:9 (Thalia) added to registry
Attribute 9876:1:10 (Urania) added to registry

AVPs from 'myavp.txt' were successfully added
```

**Step 4** If you are ready to make the imported attribute definitions take effect, restart the CSAuth and CSAdmin services.

**Caution** While CSAuth is stopped, no users are authenticated.

To restart the CSAuth, CSLog, and CSAdmin services, enter the following commands at the command prompt, allowing the computer time to perform each command:

```
net stop csauth
net start csauth
net stop cslog
net start cslog
net stop csadmin
net start csadmin
```

Cisco Secure ACS begins using the imported posture validation attributes. Attributes that have an attribute type of `in` or `in out` are available in the HTML interface when you define local policy rules.



Downloaded from www.Manualslib.com manuals search engine

# Deleting a Posture Validation Attribute Definition

The -delAVP option deletes a single posture validation attribute from Cisco Secure ACS.

**Before You Begin**

Because completing this procedure requires restarting the CSAuth service, which temporarily suspends authentication services, consider performing this procedure when demand for Cisco Secure ACS services is low.

Use the steps in Exporting Posture Validation Attribute Definitions, page D-48, to create a backup of posture validation attribute definitions. You can also use the exported attribute definition file to double-check the vendor ID, application ID, and attribute ID of the posture validation attribute you want to delete.

To delete posture validation attributes, follow these steps:

**Step 1** On the computer running Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory containing CSUtil.exe.

**Step 2** Type:

`CSUtil.exe -delavp` *vendor-ID*
*application-ID*
*attribute-ID*

For more information about vendor, application, and attribute IDs, see Posture Validation Attribute Definition File, page D-44.

CSUtil.exe prompts you to confirm the attribute deletion.

**Step 3** Examine the confirmation prompt and then do one of the following:

- If you are certain you want to delete the attribute identified by the confirmation prompt, type **Y** and press **Enter**.

**Tip** You can use the -q option to suppress the confirmation prompt.

- If you do not want to delete the attribute identified by the confirmation prompt, type N, press Enter, and return to Step 2.

CSUtil.exe deletes from its internal database the posture validation attribute you specified. In the following example, CSUtil.exe deleted an attribute with a vendor ID of 9876, an application ID of 1, and an attribute ID of 1.



Downloaded from www.Manualslib.com manuals search engine

```
CSUtil v3.3, Copyright 1997-2004, Cisco Systems Inc
Are you sure you want to delete vendor 9876; application 1; attribute 1? (y/n)
y

Vendor 9876; application 1; attribute 1 was successfully deleted
```

**Step 4** If you are ready to make the attribute deletion take effect, restart the CSAuth and CSAdmin services.

**Caution** While CSAuth is stopped, no users are authenticated.

To restart the CSAuth, CSLog, and CSAdmin services, enter the following commands at the command prompt, allowing the computer time to perform each command:

```
net stop csauth
net start csauth
net stop cslog
net start cslog
net stop csadmin
net start csadmin
```

Deleted posture validation attributes no longer are available in Cisco Secure ACS.

# Default Posture Validation Attribute Definition File

Example D-2 provides the definitions for the posture validation attributes that we provide with Cisco Secure ACS. Should you need to reset the default attributes to their original definitions, use Example D-2 to create a posture validation attribute definition file. For more information about the format of an attribute definition file, see Posture Validation Attribute Definition File, page D-44.

***Example D-2 Default Posture Validation Attribute Definitions***

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
```



Downloaded from www.Manualslib.com manuals search engine

```
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#1]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#2]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00003
attribute-name=PA-Name
attribute-profile=in out
attribute-type=string

[attr#3]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00004
attribute-name=PA-Version
attribute-profile=in out
attribute-type=version

[attr#4]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00005
attribute-name=OS-Type
attribute-profile=in out
attribute-type=string

[attr#5]
vendor-id=9
vendor-name=Cisco
application-id=1
```



Downloaded from www.Manualslib.com manuals search engine

```
application-name=PA
attribute-id=00006
attribute-name=OS-Version
attribute-profile=in out
attribute-type=version

[attr#6]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00007
attribute-name=PA-User-Notification
attribute-profile=out
attribute-type=string

[attr#7]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#8]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#9]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00006
attribute-name=ServicePacks
attribute-profile=in
attribute-type=string

[attr#10]
vendor-id=9
```



Downloaded from www.Manualslib.com manuals search engine

```
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00007
attribute-name=HotFixes
attribute-profile=in
attribute-type=string

[attr#11]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00008
attribute-name=HostFQDN
attribute-profile=in
attribute-type=string

[attr#12]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#13]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#14]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00005
attribute-name=CSAVersion
attribute-profile=in
attribute-type=version
```



Downloaded from www.Manualslib.com manuals search engine

```
[attr#15]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00009
attribute-name=CSAOperationalState
attribute-profile=in
attribute-type=unsigned integer

[attr#16]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00011
attribute-name=TimeSinceLastSuccessfulPoll
attribute-profile=in
attribute-type=unsigned integer

[attr#17]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=32768
attribute-name=CSAMCName
attribute-profile=in
attribute-type=string

[attr#18]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=32769
attribute-name=CSAStates
attribute-profile=in
attribute-type=string

[attr#19]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
```



Downloaded from www.Manualslib.com manuals search engine

```
attribute-type=unsigned integer

[attr#20]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#21]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00003
attribute-name=Software-Name
attribute-profile=in out
attribute-type=string

[attr#22]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00004
attribute-name=Software-ID
attribute-profile=in out
attribute-type=unsigned integer

[attr#23]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00005
attribute-name=Software-Version
attribute-profile=in out
attribute-type=version

[attr#24]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00006
```



Downloaded from www.Manualslib.com manuals search engine

```
attribute-name=Scan-Engine-Version
attribute-profile=in out
attribute-type=version

[attr#25]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00007
attribute-name=Dat-Version
attribute-profile=in out
attribute-type=version

[attr#26]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00008
attribute-name=Dat-Date
attribute-profile=in out
attribute-type=date

[attr#27]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00009
attribute-name=Protection-Enabled
attribute-profile=in out
attribute-type=unsigned integer

[attr#28]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00010
attribute-name=Action
attribute-profile=out
attribute-type=string

[attr#29]
vendor-id=3401
vendor-name=NAI
application-id=3
```



Downloaded from www.Manualslib.com manuals search engine

```
application-name=AV
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#30]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#31]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00003
attribute-name=Software-Name
attribute-profile=in out
attribute-type=string

[attr#32]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00004
attribute-name=Software-ID
attribute-profile=in out
attribute-type=unsigned integer

[attr#33]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00005
attribute-name=Software-Version
attribute-profile=in out
attribute-type=version

[attr#34]
vendor-id=3401
```



Downloaded from www.Manualslib.com manuals search engine

```
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00006
attribute-name=Scan-Engine-Version
attribute-profile=in out
attribute-type=version

[attr#35]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00007
attribute-name=Dat-Version
attribute-profile=in out
attribute-type=version

[attr#36]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00008
attribute-name=Dat-Date
attribute-profile=in out
attribute-type=date

[attr#37]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00009
attribute-name=Protection-Enabled
attribute-profile=in out
attribute-type=unsigned integer

[attr#38]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00010
attribute-name=Action
attribute-profile=out
attribute-type=string
```



Downloaded from www.Manualslib.com manuals search engine

```
[attr#39]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#40]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#41]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00003
attribute-name=Software-Name
attribute-profile=in out
attribute-type=string

[attr#42]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00004
attribute-name=Software-ID
attribute-profile=in out
attribute-type=unsigned integer

[attr#43]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00005
attribute-name=Software-Version
attribute-profile=in out
```



Downloaded from www.Manualslib.com manuals search engine

```
attribute-type=version

[attr#44]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00006
attribute-name=Scan-Engine-Version
attribute-profile=in out
attribute-type=version

[attr#45]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00007
attribute-name=Dat-Version
attribute-profile=in out
attribute-type=version

[attr#46]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00008
attribute-name=Dat-Date
attribute-profile=in out
attribute-type=date

[attr#47]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00009
attribute-name=Protection-Enabled
attribute-profile=in out
attribute-type=unsigned integer

[attr#48]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00010
```



Downloaded from www.Manualslib.com manuals search engine

```
attribute-name=Action
attribute-profile=out
attribute-type=string

[attr#49]
vendor-id=10000
vendor-name=out
application-id=1
application-name=CNAC
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=string

[attr#50]
vendor-id=10000
vendor-name=out
application-id=1
application-name=CNAC
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=string

[attr#51]
vendor-id=10000
vendor-name=out
application-id=1
application-name=CNAC
attribute-id=00003
attribute-name=Reason
attribute-profile=out
attribute-type=string
```



Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

# VPDN Processing

Cisco Secure ACS for Windows Server supports authentication forwarding of virtual private dial-up network (VPDN) requests. There are two basic types of "roaming" users: Internet and intranet; VPDN addresses the requirements of roaming intranet users. This chapter provides information about the VPDN process and how it affects the operation of Cisco Secure ACS.

## VPDN Process

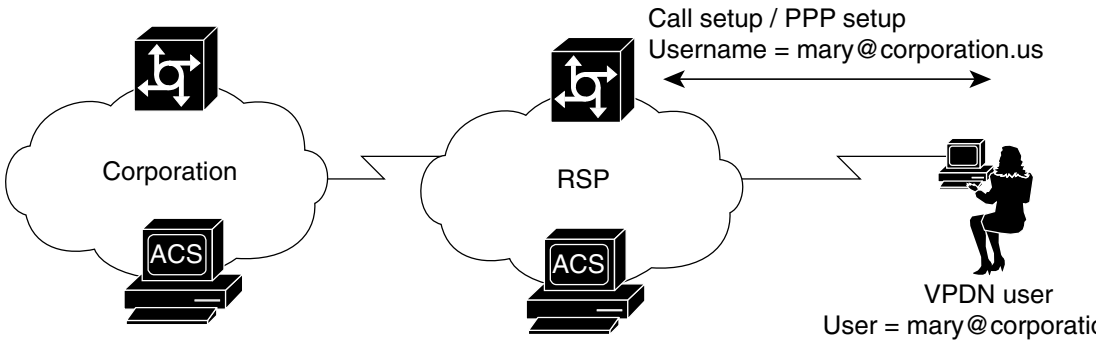
This section describes the steps for processing VPDN requests in a standard environment.

1. A VPDN user dials in to the network access server (NAS) of the regional service provider (RSP). The standard call/point-to-point protocol (PPP) setup is done. A username and password are sent to the NAS in the format username@domain (for example, mary@corporation.us). See Figure E-1.



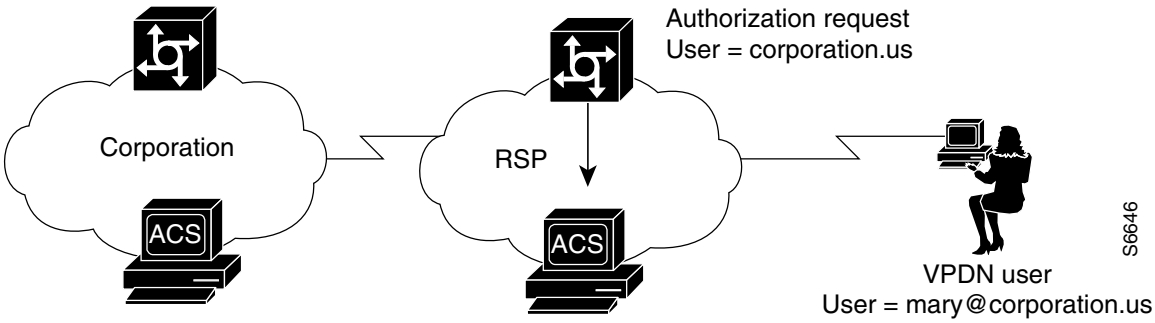
Downloaded from www.Manualslib.com manuals search engine

*Figure E-1 VPDN User Dials In*




2. If VPDN is enabled, the NAS assumes that the user is a VPDN user. The NAS strips off the "username@" (mary@) portion of the username and authorizes (not authenticates) the domain portion (corporation.us) with the ACS. See Figure E-2.

*Figure E-2 NAS Attempts to Authorize Domain*

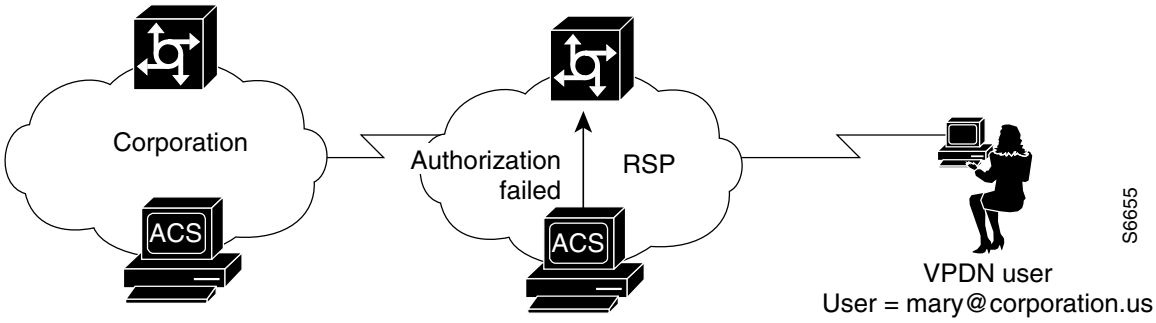



3. If the domain authorization fails, the NAS assumes the user is not a VPDN user. The NAS then authenticates (not authorizes) the user as if the user is a standard non-VPDN dial user. See Figure E-3.



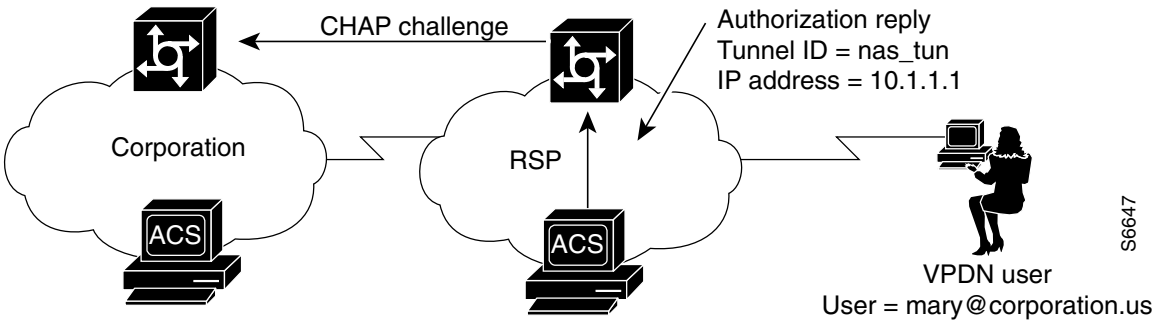
Downloaded from www.Manualslib.com manuals search engine

*Figure E-3 Authorization of Domain Fails*




If the ACS authorizes the domain, it returns the Tunnel ID and the IP address of the home gateway (HG); these are used to create the tunnel. See Figure E-4.

*Figure E-4 ACS Authorizes Domain*

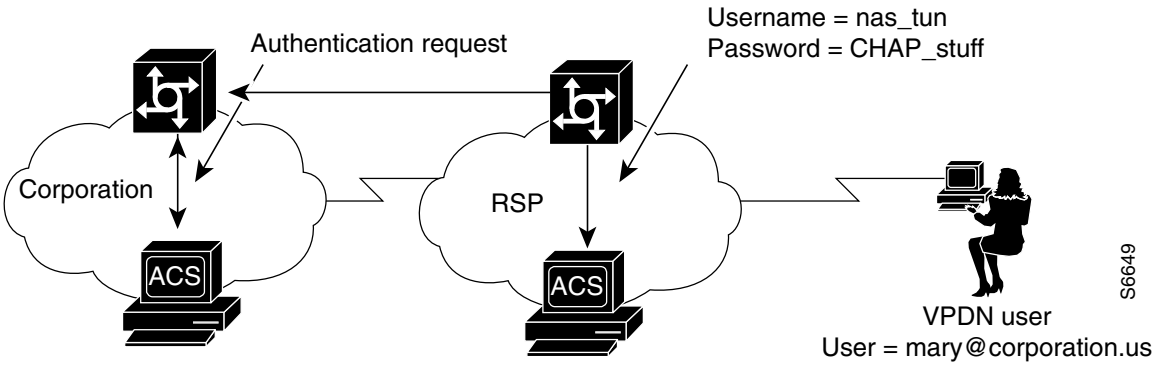



4. The HG uses its ACS to authenticate the tunnel, where the username is the name of the tunnel (nas_tun). See Figure E-5.



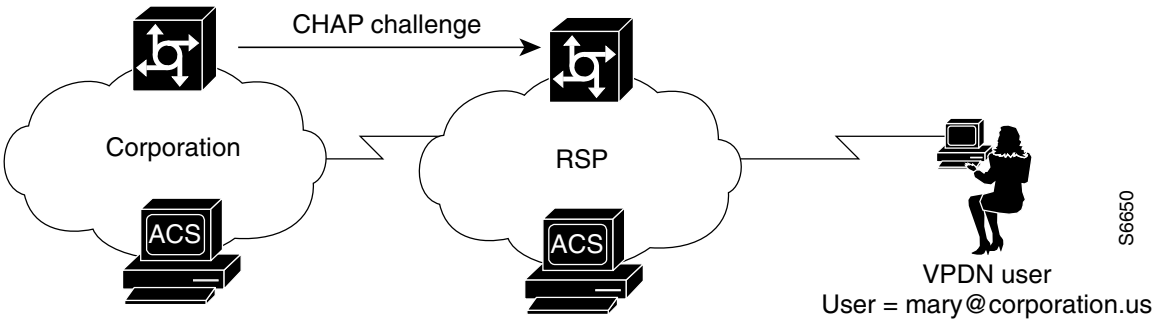
Downloaded from www.Manualslib.com manuals search engine

*Figure E-5 HG Authenticates Tunnel with ACS*




5. The HG now authenticates the tunnel with the NAS, where the username is the name of the HG. This name is chosen based on the name of the tunnel, so the HG might have different names depending on the tunnel being set up. See Figure E-6.

*Figure E-6 HG Authenticates Tunnel with the NAS*

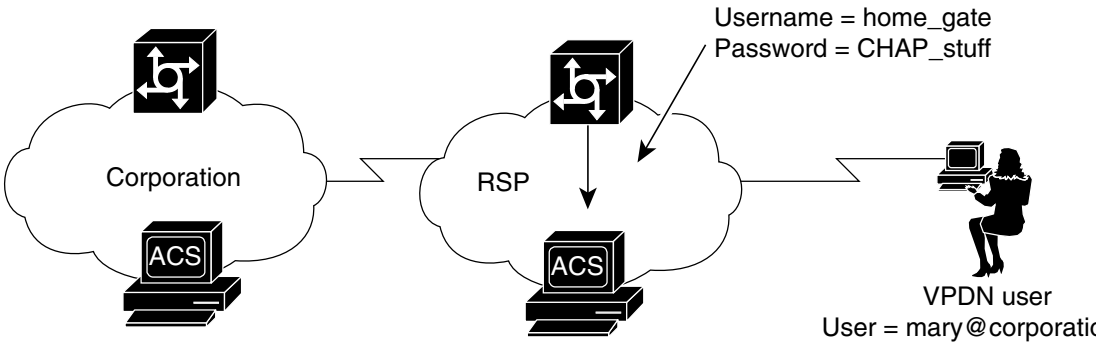



6. The NAS now uses its ACS to authenticate the tunnel from the HG. See Figure E-7.



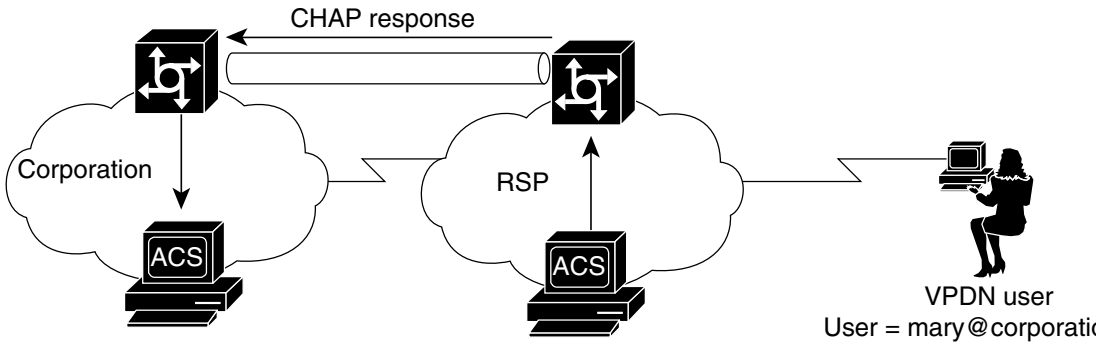
Downloaded from www.Manualslib.com manuals search engine

*Figure E-7 NAS Authenticates Tunnel with ACS*




7. After authenticating, the tunnel is established. Now the actual user (mary@corporation.us) must be authenticated. See Figure E-8.

*Figure E-8 VPDN Tunnel is Established*

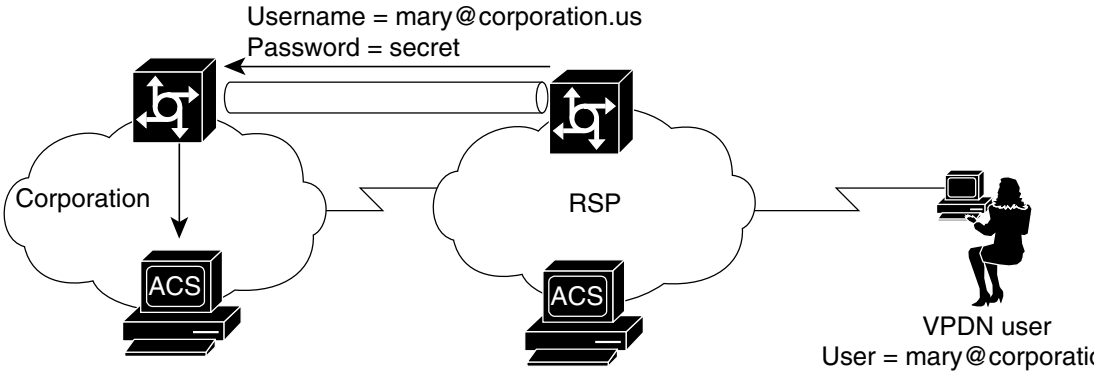



8. The HG now authenticates the user as if the user dialed directly in to the HG. The HG might now challenge the user for a password. The Cisco Secure ACS at RSP can be configured to strip off the @ and domain before it passes the authentication to the HG. (The user is passed as mary@corporation.us.) The HG uses its ACS to authenticate the user. See Figure E-9.



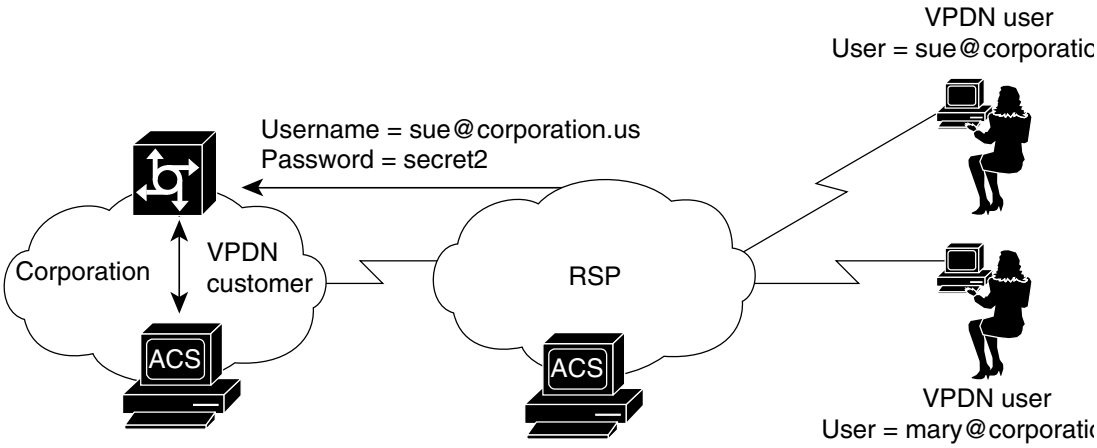
Downloaded from www.Manualslib.com manuals search engine

*Figure E-9 HG Uses ACS to Authenticate User*




9. If another user (sue@corporation.us) dials in to the NAS while the tunnel is up, the NAS does not repeat the entire authorization/authentication process. Instead, it passes the user through the existing tunnel to the HG. See Figure E-10.

*Figure E-10 Another User Dials In While Tunnel is Up*






Downloaded from www.Manualslib.com manuals search engine

# RDBMS Synchronization Import Definitions

RDBMS synchronization import definitions are a listing of the action codes allowable in an accountActions table. The RDBMS Synchronization feature of Cisco Secure Access Control Server (ACS) for Windows Server uses a table named “accountActions” as input for automated or manual updates of the CiscoSecure user database. For more information about the RDBMS Synchronization feature and accountActions, see RDBMS Synchronization, page 9-25.

This chapter contains the following topics:


- accountActions Specification, page F-1
- Action Codes, page F-4
- Cisco Secure ACS Attributes and Action Codes, page F-32
- An Example of accountActions, page F-36


## accountActions Specification

Whether you create accountActions by hand in a text editor or through automation using a third-party system that writes to accountActions, you must adhere to the accountActions specification and must only use the action codes detailed in Action Codes, page F-4. Otherwise, RDBMS Synchronization may import incorrect information into the CiscoSecure user database or may fail to occur at all.



Downloaded from www.Manualslib.com manuals search engine

# accountActions Format

Each row in accountActions has 14 fields (or columns). Table F-1 lists the fields that compose accountActions. Table F-1 also reflects the order in which the fields appear in accountActions.

The one-letter or two-letter abbreviations given in the Mnemonic column are a shorthand notation used to indicate required fields for each action code in Action Codes, page F-4.

To see an example accountActions, see An Example of accountActions, page F-36.

***Table F-1 accountActions Fields***

| Field Name | Mnemonic | Type | Size (Max. Length) | Comments |
|---|---|---|---|---|
| SequenceId | SI | AutoNumber | 32 | The unique action ID. |
| Priority | P | Integer | 1 | The priority with which this update is to be treated. 0 is the lowest priority. |
| UserName | UN | String | 32 | The name of the user to which the transaction applies. |
| GroupName | GN | String | 32 | The name of the group to which the transaction applies. |
| Action | A | Number | $0\text{-}2^{16}$ | The Action required. (See Action Codes, page F-4.) |
| ValueName | VN | String | 255 | The name of the parameter to change. |
| Value1 | V1 | String | 255 | The new value (for numeric parameters, this is a decimal string). |
| Value2 | V2 | String | 255 | The name of a TACACS+ protocol; for example, “ip” or RADIUS VSA Vendor ID. |
| Value3 | V3 | String | 255 | The name of a TACACS+ service; for example, “ppp” or the RADIUS VSA attribute number. |
| DateTime | DT | DateTime | — | The date/time the Action was created. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-1 accountActions Fields (continued)*

| Field Name | Mnemonic | Type | Size (Max. Length) | Comments |
|---|---|---|---|---|
| MessageNo | MN | Integer | — | Used to number related transactions for audit purposes. |
| ComputerNames | CN | String | 32 | RESERVED by CSDBSync. |
| AppId | AI | String | 255 | The type of configuration parameter to change. |
| Status | S | Number | 32 | TRI-STATE:0=not processed, 1=done, 2=failed. This should normally be set to 0. |

# accountActions Mandatory Fields

For all actions, the following three fields cannot be empty and must have a valid value:

- Action
- DateTime
- SequenceID

In addition to the three required fields above, the UserName and GroupName fields are also often required to have a valid value:

- If a transaction is acting upon a user account, a valid value is required in the UserName field.
- If a transaction is acting upon a group, a valid value is required in the GroupName field.
- If a transaction is acting upon AAA client configuration, neither the UserName field nor the GroupName field require a value.

**Note** The UserName and GroupName fields are mutually exclusive; only one of these two fields can have a value and neither field is always required.



Downloaded from www.Manualslib.com manuals search engine

## accountActions Processing Order

Cisco Secure ACS reads rows from accountActions and processes them in a specific order. Cisco Secure ACS determines the order first by the values in the Priority fields (mnemonic: P) and then by the values in the Sequence ID fields (mnemonic: SI). Cisco Secure ACS processes the rows with the highest Priority field. The lower the number in the Priority field, the higher the priority. For example, if row A has the value 1 in its Priority field and row B has the value 2 in its Priority field, Cisco Secure ACS would process row A first, regardless of whether row B has a lower sequence ID or not. If rows have an equal priority, Cisco Secure ACS processes them by their sequence ID, with the lowest sequence ID processed first.

Thus, the Priority field (P) enables transactions of higher importance to occur first, such as deleting a user or changing a password. In the most common implementations of RDBMS Synchronization, a third-party system writes to accountActions in batch mode, with all actions (rows) assigned a priority of zero (0).

**Note** When changing transaction priorities, be careful that they are processed in the correct order; for example, a user account must be created before the user password is assigned.

You can use the MessageNo field (mnemonic: MN) to associate related transactions, such as the addition of a user and subsequent actions to set password values and status. You can use the MessageNo field to create an audit trail for a third-party system that writes to accountActions.

# Action Codes

This section provides the action codes valid for use in the Action field (mnemonic: A) of accountActions. The Required column uses the field mnemonic names to indicate which fields should be completed, except for the mandatory fields, which are assumed. For more information about the mnemonic names of accountActions fields, see Table F-1. For more information about the mandatory fields, see accountActions Mandatory Fields, page F-3.



Downloaded from www.Manualslib.com manuals search engine

If an action can be applied to either a user or group, "UN|GN" appears, using the vertical bar to indicate that either one of the two fields is required. To make the action affect only the user, leave the group name empty; to make the action affect only the group, leave the user name empty.

This section contains the following topics:


- Action Codes for Setting and Deleting Values, page F-5
- Action Codes for Creating and Modifying User Accounts, page F-7
- Action Codes for Initializing and Modifying Access Filters, page F-14
- Action Codes for Modifying TACACS+ and RADIUS Group and User Settings, page F-19
- Action Codes for Modifying Network Configuration, page F-25


# Action Codes for Setting and Deleting Values

The two most fundamental action codes are SET_VALUE (action code: 1) and DELETE_VALUE (action code: 2), described in Table F-2.

The SET_VALUE (action code: 1) and DELETE_VALUE (action code: 2) actions, described in Table F-2, instruct RDBMS Synchronization to assign a value to various internal attributes in Cisco Secure ACS. Unless asked to use these action codes for other purposes by a Cisco representative, you can only use these action codes for assigning values to user-defined fields (see User-Specific Attributes, page F-32).



Downloaded from www.Manualslib.com manuals search engine

*Table F-2 Action Codes for Setting and Deleting Values*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 1 | SET_VALUE | UN\|GN, AI, VN, V1, V2 | Sets a value (V1) named (VN) of type (V2) for App ID (AI).<br>App IDs (AI) can be one of the following:<br>• APP_CSAUTH<br>• APP_CSTACACS<br>• APP_CSRADIUS<br>• APP_CSADMIN<br>Value types (V2) can be one of the following:<br>• **TYPE_BYTE**—Single 8-bit number.<br>• **TYPE_SHORT**—Single 16-bit number.<br>• **TYPE_INT**—Single 32-bit number.<br>• **TYPE_STRING**—Single string.<br>• **TYPE_ENCRYPTED_STRING**—Single string to be saved encrypted.<br>• **TYPE_MULTI_STRING**—Tab-separated set of substrings.<br>• **TYPE_MULTI_INT**—Tab-separated set of 32-bit numbers.<br>For example:<br>`UN = "fred"`<br>`AI = "APP_CSAUTH"`<br>`VN = "My Value"`<br>`V2 = "TYPE_MULTI_STRING"`<br>`V1 = "str1`*tab*`str2`*tab*`str3"` |
| 2 | DELETE_VALUE | UN\|GN, AI, VN | Deletes value (VN) for App ID (AI) and user (UN) or group (GN). |



Downloaded from www.Manualslib.com manuals search engine

# Action Codes for Creating and Modifying User Accounts

Table F-3 lists the action codes for creating, modifying, and deleting user accounts.

**Note** Before you can modify a user account, such as assigning a password, you must create the user account, either in the HTML interface or by using the ADD_USER action (action code: 100).

Transactions using these codes affect the configuration displayed in the User Setup section of the HTML interface. For more information about the User Setup section, see Chapter 7, "User Management".

*Table F-3 User Creation and Modification Action Codes*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 100 | ADD_USER | UN\|GN, V1 | Creates a user (32 characters maximum). V1 is used as the initial password. Optionally, the user can also be assigned to a group. |
| 101 | DELETE_USER | UN | Removes a user. |
| 102 | SET_PAP_PASS | UN, V1 | Sets the PAP password for a user (64 ASCII characters maximum). CHAP/ARAP will also default to this. |
| 103 | SET_CHAP_PASS | UN, V1 | Sets the CHAP/ARAP password for a user (64 characters maximum). |
| 104 | SET_OUTBOUND_CHAP_PASS | UN, V1 | Sets the CHAP/ARAP password for a user (32 characters maximum). |



Downloaded from www.Manualslib.com manuals search engine

*Table F-3 User Creation and Modification Action Codes (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 105 | SET_T+_ENABLE_ PASS | UN, VN, V1, V2, V3 | Sets the TACACS+ enable password (V1) (32 characters maximum) and Max Privilege level (V2) (0-15).<br>The enable type (V3) should be one of the following:<br>• **ENABLE_LEVEL_AS_GROUP**—Max privilege taken from group setting.<br>• **ENABLE_LEVEL_NONE**—No T+ enable configured.<br>• **ENABLE_LEVEL_STATIC**—Value set in V2 used during enable level check.<br>You can use VN to link the enable password to an external authenticator, as per action 108 SET_PASS_TYPE. |
| 106 | SET_GROUP | UN, GN | Sets the Cisco Secure ACS group assignment of the user. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-3 User Creation and Modification Action Codes (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 108 | SET_PASS_TYPE | UN\|GN, V1 | Sets the password type of the user. This can be one of the CiscoSecure user database password types or any of the external databases supported:<br>• **PASS_TYPE_CSDB**—CSDB internal password.<br>• **PASS_ TYPE_CSDB_UNIX**—CSDB internal password (UNIX encrypted).<br>• **PASS_TYPE_NT**—External Windows user database password.<br>• **PASS_TYPE_NDS**—External Novell database password.<br>• **PASS_TYPE_LDAP**—External generic LDAP database password.<br>• **PASS_TYPE_LEAP**—External LEAP proxy RADIUS server database password.<br>• **PASS_TYPE_RADIUS_TOKEN**—External RADIUS token server database password. |
| 109 | REMOVE_PASS_ STATUS | UN,V1 | Removes a password status flag. This results in the status states being linked in a logical XOR condition. V1 should contain one of the following:<br>• **PASS_STATUS_EXPIRES**—Password expires on a given date.<br>• **PASS_STATUS_NEVER**—Password never expires.<br>• **PASS_STATUS_WRONG**—Password expires after a given number of login attempts using the wrong password.<br>• **PASS_STATUS_DISABLED**—The account has been disabled. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-3 User Creation and Modification Action Codes (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 110 | ADD_PASS_STATUS | UN, V1 | Defines how a password should be expired by Cisco Secure ACS. To set multiple password states for a user, use multiple instances of this action. This results in the status states being linked in a logical XOR condition. V1 should contain one of the following:<br>• **PASS_STATUS_EXPIRES**—Password expires on a given date.<br>• **PASS_STATUS_NEVER**—Password never expires.<br>• **PASS_STATUS_WRONG**—Password expires after a given number of login attempts using the wrong password.<br>• **PASS_STATUS_RIGHT**—Password expires after a given number of login attempts using the correct password.<br>• **PASS_STATUS_DISABLED**—The account has been disabled. |
| 112 | SET_PASS_EXPIRY_ WRONG | UN,V1 | Sets the maximum number of bad authentications allowed (automatic reset on good password if not exceeded) and reset current count. |
| 113 | SET_PASS_EXPIRY_ DATE | UN,V1 | Sets the date on which the account expires. The date format should be YYYYMMDD. |
| 114 | SET_MAX_SESSIONS | UN\|GN, V1 | Sets the maximum number of simultaneous sessions for a user or group. V1 should contain one of the following values:<br>• MAX_SESSIONS_UNLIMITED<br>• MAX_SESSIONS_AS_GROUP<br>• 1-65534 |



Downloaded from www.Manualslib.com manuals search engine

*Table F-3 User Creation and Modification Action Codes (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 115 | SET_MAX_ SESSIONS_GROUP_ USER | GN,V1 | Sets the max sessions for a user of the group to one of the following values:<br>• MAX_SESSIONS_UNLIMITED<br>• 1-65534 |
| 260 | SET_QUOTA | VN,V1, V2 | Sets a quota for a user or group.<br>VN defines the quota type. Valid values are:<br>• **online time**—The quota limits the user or group by the number of seconds logged in to the network for the period defined in V2.<br>• **sessions**—The quota limits the user or group by the number of sessions on the network for the period defined in V2.<br>V1 defines the quota. If VN is set to sessions, V1 is the maximum number of sessions in the period defined in V2. If VN is set to online time, V1 is the maximum number of seconds.<br>V2 holds the period for the quota. Valid values are:<br>• **QUOTA_PERIOD_DAILY**—The quota is enforced in 24-hour cycles, from 12:01 A.M. to midnight.<br>• **QUOTA_PERIOD_WEEKLY**—The quota is enforced in 7-day cycles, from 12:01 A.M. Sunday until midnight Saturday.<br>• **QUOTA_PERIOD_MONTHLY**—The quota is enforced in monthly cycles, from 12:01 A.M. on the first of the month until midnight on the last day of the month.<br>• **QUOTA_PERIOD_ABSOLUTE**—The quota is enforced in an ongoing basis, without an end. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-3 User Creation and Modification Action Codes (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 261 | DISABLE_QUOTA | UN\|GN, VN | Disables a group or user usage quota.<br>VN defines the quota type. Valid values are:<br>• **online time**—The quota limits the user or group by the number of seconds logged in to the network for the period defined in V2.<br>• **sessions**—The quota limits the user or group by the number of sessions on the network for the period defined in V2. |
| 262 | RESET_COUNTERS | UN\|GN | Resets usage quota counters for a user or group. |
| 263 | SET_QUOTA_APPLY_TYPE | V1 | Defines whether a user usage quota is determined by the user group quota or by a quota unique to the user. V1 makes this specification. Valid values for V1 are:<br>• ASSIGNMENT_FROM_USER<br>• ASSIGNMENT_FROM_GROUP |



Downloaded from www.Manualslib.com manuals search engine

*Table F-3 User Creation and Modification Action Codes (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 270 | SET_DCS_TYPE | UN\|GN, VN,V1, Optional-ly V2 | Sets the type of device command set (DCS) authorization for a group or user.<br>VN defines the service. Valid service types are:<br>• **shell**—Cisco IOS shell command authorization.<br>• **pixshell**—Cisco PIX command authorization.<br>**Note** If additional DCS types have been added to your Cisco Secure ACS, you can find the valid value in the Interface Configuration page for TACACS+ (Cisco IOS). The valid values appear in parentheses after the service title, such as `PIX Shell (pixshell)`.<br>V1 defines the assignment type. The valid values for VN are:<br>• **none**—Sets no DCS for the user or group.<br>• **as group**—For users only, this value signifies that the user DCS settings for the service specified should be the same as the user group DCS settings.<br>• **static**—Sets a DCS for the user or group for all devices enabled to perform command authorization for the service specified.<br>If V1 is set to static, V2 is required and must contain the name of the DCS to assign to the user or group for the given service.<br>• **ndg**—Specifies that command authorization for the user or group is to be done on a per-NDG basis. Use action 271 to add DCS to NDG mappings for the user or group.<br>**Note** Changing a user or group assignment type (V1) results in clearing previous data, including NDG to DCS mappings (defined by action 271). |



Downloaded from www.Manualslib.com manuals search engine

*Table F-3 User Creation and Modification Action Codes (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 271 | SET_DCS_NDG_MAP | UN\|GN, VN,V1, V2 | Use this action code to map between the device command set and the NDG when the assignment type specified by a 270 action code is `ndg`.<br>VN defines the service. Valid service types are:<br>• **shell**—Cisco IOS shell command authorization.<br>• **pixshell**—Cisco PIX command authorization.<br>**Note** If additional DCS types have been added to your Cisco Secure ACS, you can find the valid value in the Interface Configuration page for TACACS+ (Cisco IOS). The valid values appear in parentheses after the service title, such as `PIX Shell (pixshell)`.<br>V1 defines the name of the NDG. Use the name of the NDG as it appears in the HTML interface. For example, if you have configured an NDG named "East Coast NASes" and want to use action 271 to apply a DCS to that NDG, V1 should be "East Coast NASes".<br>V2 defines the name of the DCS. Use the name of the DCS as it appears in the HTML interface. For example, if you have configured a DCS named "Tier2 PIX Admin DCS" and want to use action 271 to apply it to an NDG, V2 should be "Tier2 PIX Admin DCS". |

# Action Codes for Initializing and Modifying Access Filters

Table F-4 lists the action codes for initializing and modifying AAA client access filters. AAA client access filters control Telnet access to a AAA client. Dial access filters control access by dial-up users.



Downloaded from www.Manualslib.com manuals search engine

Transactions using these codes affect the configuration displayed in the User Setup and Group Setup sections of the HTML interface. For more information about the User Setup section, see Chapter 7, "User Management". For more information about the Group Setup section, see Chapter 6, "User Group Management".

*Table F-4 Action Codes for Initializing and Modifying Access Filters*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 120 | INIT_NAS_ACCESS_CONTROL | UN\|GN,V1 | Clears the AAA client access filter list and initialize permit/deny for any forthcoming filters. V1 should be one of the following values:<br>• ACCESS_PERMIT<br>• ACCESS DENY |
| 121 | INIT_DIAL_ACCESS_CONTROL | UN\|GN,V1 | Clears the dial-up access filter list and initialize permit/deny for any forthcoming filters. V1 should be one of the following values:<br>• ACCESS_PERMIT<br>• ACCESS DENY |
| 122 | ADD_NAS_ACCESS_FILTER | UN\|GN,V1 | Adds a AAA client filter for the user\|group.<br>V1 should contain a single (AAA client name, AAA client port, remote address, CLID) tuple; for example:<br>`NAS01,tty0,0898-69696969`<br>Optionally, the AAA client name can be "All AAA clients" to specify that the filter applies to all configured AAA clients and an asterisk (*) to represent all ports. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-4 Action Codes for Initializing and Modifying Access Filters (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 123 | ADD_DIAL_ACCESS_FILTER | UN\|GN, V1, V2 | Adds a dial-up filter for the user\|group.<br>V1 should contain one of the following values:<br>• Calling station ID<br>• Called station ID<br>• Calling and called station ID; for example:<br>`01732-875374,0898-69696969`<br>• AAA client IP address, AAA client port; for example:<br>`10.45.6.123,tty0`<br>V2 should contain the filter type as one of the following values:<br>• **CLID**—The user is filtered by the calling station ID.<br>• **DNIS**—The user is filtered by the called station ID.<br>• **CLID/DNIS**—The user is filtered by both calling and called station IDs.<br>• **AAA client/PORT**—The user is filtered by AAA client IP and AAA client port address. |
| 130 | SET_TOKEN_CACHE_SESSION | GN, V1 | Enables/disables token caching for an entire session; V1 is 0=disable, 1=enable. |
| 131 | SET_TOKEN_CACHE_TIME | GN, V1 | Sets the duration that tokens are cached. V1 is the token cache duration in seconds. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-4 Action Codes for Initializing and Modifying Access Filters (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 140 | SET_TODDOW_ACCESS | UN\|GN, V1 | Sets periods during which access is permitted. V1 contains a string of 168 characters. Each character represents a single hour of the week. A "1" represents an hour that is permitted, while a "0" represents an hour that is denied. If this parameter is not specified for a user, the group setting applies. The default group setting is "111111111111" and so on. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-4 Action Codes for Initializing and Modifying Access Filters (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 150 | SET_STATIC_IP | UN, V1, V2 | Configures the (TACACS+ and RADIUS) IP address assignment for this user.<br>V1 holds the IP address in the following format:<br>*xxx.xxx.xxx.xxx*<br>V2 should be one of the following:<br>• **ALLOC_METHOD_STATIC**—The IP address in V1 is assigned to the user in the format xxx.xxx.xxx.xxx.<br>• **ALLOC_METHOD_NAS_POOL**—The IP pool named in V1 (configured on the AAA client) will be assigned to the user.<br>• **ALLOC_METHOD_AAA_POOL**—The IP pool named in V1 (configured on the AAA server) will be assigned to the user.<br>• **ALLOC_METHOD_CLIENT**—The dial-in client will assign its own IP address.<br>• **ALLOC_METHOD_AS_GROUP**—The IP address assignment configured for the group will be used. |
| 151 | SET_CALLBACK_NO | UN\|GN, V1 | Sets the callback number for this user or group (TACACS+ and RADIUS). V1 should be one of the following:<br>• **Callback number**—The phone number the AAA client is to call back.<br>• **none**—No callback is allowed.<br>• **roaming**—The dial-up client determines the callback number.<br>• **as group**—Use the callback string or method defined by the group. |



Downloaded from www.Manualslib.com manuals search engine

# Action Codes for Modifying TACACS+ and RADIUS Group and User Settings

Table F-5 lists the action codes for creating, modifying, and deleting TACACS+ and RADIUS settings for Cisco Secure ACS groups and users. In the event that Cisco Secure ACS has conflicting user and group settings, user settings always override group settings.

Transactions using these codes affect the configuration displayed in the User Setup and Group Setup sections of the HTML interface. For more information about the User Setup section, see Chapter 7, "User Management". For more information about the Group Setup section, see Chapter 6, "User Group Management".

*Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 161 | DEL_RADIUS_ATTR | UN\|GN, VN, Optionally V2, V3 | Deletes the named RADIUS attribute for the group or user, where:<br>• VN = "Vendor-Specific"<br>• V2 = IETF vendor ID<br>• V3 = VSA attribute ID<br>For example, to specify the Cisco IOS/PIX vendor ID and the Cisco AV Pair:<br>`VN = "Vendor-Specific"`<br>`V2 = "9"`<br>`V3 = "1"` |



Downloaded from www.Manualslib.com manuals search engine

*Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 163 | ADD_RADIUS_ ATTR | UN\|GN, VN, V1, Optionally V2, V3 | Adds to the attribute named (VN) the value (V1) for the user/group (UN\|GN). For example, to set the IETF RADIUS Reply-Message attribute (attr. 18) for a group:<br>`GN = "Group 1"`<br>`VN = "Reply-Message"`<br>`V1 = "Greetings"`<br>As another example, to set the IETF RADIUS Framed-IP-Address attribute (attr. 9) for a user:<br>`UN = "fred"`<br>`VN = "Framed-IP-Address"`<br>`V1 = "10.1.1.1"`<br>To add a vendor-specific attribute (VSA), set VN = "Vendor-Specific" and use V2 and V3 as follows:<br>• V2 = IETF vendor ID<br>• V3 = VSA attribute ID<br>For example, to add the Cisco IOS/PIX RADIUS cisco-av-pair attribute with a value of "addr-pool=pool1":<br>`VN="Vendor-Specific"`<br>`V1 = "addr-pool=pool1"`<br>`V2 = "9"`<br>`V3 = "1"`<br>RADIUS attribute values can be one of the following:<br>• INTEGER<br>• TIME<br>• IP ADDRESS<br>• STRING |



Downloaded from www.Manualslib.com manuals search engine

*Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 170 | ADD_TACACS_ SERVICE | UN\|GN, VN, V1, V3, Optionally V2 | Permits the service for that user or group of users. For example:<br>`GN = "Group 1"`<br>`V1 = "ppp"`<br>`V2 = "ip"`<br>or<br>`UN = "fred"`<br>`V1 = "ppp"`<br>`V2 = "ip"`<br>or<br>`UN = "fred"`<br>`V1= "exec"` |
| 171 | REMOVE_TACACS_ SERVICE | UN\|GN, V1<br>Optionally V2 | Denies the service for that user or group of users. For example:<br>`GN = "Group 1"`<br>`V1 = "ppp"`<br>`V2 = "ip"`<br>or<br>`UN = "fred"`<br>`V1 = "ppp"`<br>`V2 = "ip"`<br>or<br>`UN = "fred"`<br>`V1 = "exec"`<br>This also resets the valid attributes for the service. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 172 | ADD_TACACS_ATTR | UN\|GN, VN, V1, V3<br>Optionally V2 | Sets a service-specific attribute. The service must already have been permitted either via the HTML interface or using Action 170:<br>`GN = "Group 1"`<br>`VN = "routing"`<br>`V1 = "ppp"`<br>`V2 = "ip"`<br>`V3 = "true"`<br>or<br>`UN = "fred"`<br>`VN = "route"`<br>`V1 = "ppp"`<br>`V2 = "ip"`<br>`V3 = 10.2.2.2` |
| 173 | REMOVE_TACACS_ATTR | UN\|GN, VN, V1<br>Optionally V2 | Removes a service-specific attribute:<br>`GN = "Group 1"`<br>`V1 = "ppp"`<br>`V2 = "ip"`<br>`VN = "routing"`<br>or<br>`UN = "fred"`<br>`V1 = "ppp"`<br>`V2 = "ip"`<br>`VN = "route"` |



Downloaded from www.Manualslib.com manuals search engine

*Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 174 | ADD_IOS_ COMMAND | UN\|GN, VN, V1 | Authorizes the given Cisco IOS command and determines if any arguments given to the command are to be found in a defined set or are not to be found in a defined set. The defined set is created using Actions 176 and 177:<br>`GN = "Group 1"`<br>`VN = "telnet"`<br>`V1 = "permit"`<br>or<br>`UN = "fred"`<br>`VN = "configure"`<br>`V1 = "deny"`<br>The first example permits the Telnet command to be authorized for users of Group 1. Any arguments can be supplied to the Telnet command as long as they are not matched against any arguments defined via Action 176.<br>The second example permits the **configure** command to be authorized for user fred, but only if the arguments supplied are permitted by the filter defined by a series of Action 176. |
| 175 | REMOVE_IOS_ COMMAND | UN\|GN, VN | Removes command authorization for the user or group:<br>`GN = "Group 1"`<br>`VN = "telnet"`<br>or<br>`UN = "fred"`<br>`VN = "configure"`<br>Users of Group 1 can no longer use the Cisco IOS **telnet** command.<br>User fred can no longer use the **configure** command. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 176 | ADD_IOS_ COMMAND_ARG | UN\|GN, VN, V1, V2 | Specifies a set of command-line arguments that are either permitted or denied for the Cisco IOS command contained in VN. The command must have already been added via Action 174:<br>`GN = "Group 1"`<br>`VN = "telnet"`<br>`V1 = "permit"`<br>`V2 = "10.1.1.2"`<br>or<br>`UN = "fred"`<br>`VN = "show"`<br>`V1 = "deny"`<br>`V2 = "run"`<br>The first example will allow the **telnet** command with argument 10.1.1.2 to be used by any user in Group 1.<br>The second example ensures that user fred cannot issue the Cisco IOS command **show run**. |
| 177 | REMOVE_IOS_ COMMAND_ARG | UN\|GN, VN, V2 | Removes the permit or deny entry for the given Cisco IOS command argument:<br>`GN = "Group 1"`<br>`VN = "telnet"`<br>`V2 = "10.1.1.1"`<br>or<br>`UN = "fred"`<br>`VN = "show"`<br>`V2 = "run"` |



Downloaded from www.Manualslib.com manuals search engine

*Table F-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 178 | SET_PERMIT_DENY_UNMATCHED_IOS_COMMANDS | UN\|GN, V1 | Sets unmatched Cisco IOS command behavior. The default is that any Cisco IOS commands not defined via a combination of Actions 174 and 175 will be denied. This behavior can be changed so that issued Cisco IOS commands that do not match any command/command argument pairs are authorized:<br>`GN = "Group 1"`<br>`V1 = "permit"`<br>or<br>`UN = "fred"`<br>`V1 = "deny"`<br>The first example will permit any command not defined by Action 174. |
| 179 | REMOVE_ALL_IOS_COMMANDS | UN\|GN | This action removes all Cisco IOS commands defined for a particular user or group. |
| 210 | RENAME_GROUP | GN,V1 | Renames an existing group to the name supplied in V1. |
| 211 | RESET_GROUP | GN | Resets a group back to the factory default. |
| 212 | SET_VOIP | GN, V1 | Enables or disables Voice over IP (VoIP) support for the group named, as follows:<br>• GN = name of group<br>• V1 = ENABLE or DISABLE |

# Action Codes for Modifying Network Configuration

Table F-6 lists the action codes for adding AAA clients, AAA servers, network device groups, and proxy table entries. Transactions using these codes affect the configuration displayed in the Network Configuration section of the HTML interface. For more information about the Network Configuration section, see Chapter 4, "Network Configuration".



Downloaded from www.Manualslib.com manuals search engine

*Table F-6 Action Codes for Modifying Network Configuration*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 220 | ADD_NAS | VN, V1, V2, V3 | Adds a new AAA client (named in VN) with an IP address (V1), shared secret key (V2), and vendor (V3). Valid vendors are as follows:<br>• **VENDOR_ID_IETF_RADIUS**—For IETF RADIUS.<br>• **VENDOR_ID_CISCO_RADIUS**—For Cisco IOS/PIX RADIUS.<br>• **VENDOR_ID_CISCO_TACACS**—For Cisco TACACS+.<br>• **VENDOR_ID_ASCEND_RADIUS**—For Ascend RADIUS.<br>• **VENDOR_ID_ALTIGA_RADIUS**—For Cisco VPN 3000 RADIUS.<br>• **VENDOR_ID_COMPATIBLE_RADIUS**—For Cisco VPN 5000 RADIUS.<br>• **VENDOR_ID_AIRONET_RADIUS**—For Cisco Aironet RADIUS.<br>• **VENDOR_ID_NORTEL_RADIUS**—For Nortel RADIUS.<br>• **VENDOR_ID_JUNIPER_RADIUS**—For Juniper RADIUS.<br>• **VENDOR_ID_CBBMS_RADIUS**—For Cisco BBMS RADIUS.<br>For example:<br>`VN = AS5200-11`<br>`V1 = 192.168.1.11`<br>`V2 = byZantine32`<br>`V3 = VENDOR_ID_CISCO_RADIUS` |



Downloaded from www.Manualslib.com manuals search engine

*Table F-6 Action Codes for Modifying Network Configuration (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 221 | SET_NAS_FLAG | VN, V1 | Sets one of the per-AAA client flags (V1) for the named AAA client (VN). Use the action once for each flag required. Valid values for per-AAA client flags are as follows:<br>• FLAG_SINGLE_CONNECT<br>• FLAG_LOG_KEEP_ALIVE<br>• FLAG_LOG_TUNNELS |
| 222 | DEL_HOST | VN | Deletes the named AAA client (VN). |
| 223 | ADD_NAS_BY_IETF_CODE | VN,V1, V2, V3 | Adds a new AAA client (named in VN) with an IP address (V1), shared secret key (V2), and the enterprise code for the vendor (V3). |
| 230 | ADD_AAA_SERVER | VN, V1, V2 | Adds a new AAA server named (VN) with IP address (V1), shared secret key (V2). |
| 231 | SET_AAA_TYPE | VN, V1 | Sets the AAA server type for server (VN) to value in V1, which should be one of the following:<br>• TYPE_ACS<br>• TYPE_TACACS<br>• TYPE_RADIUS<br>• The default is AAA_SERVER_TYPE_ACS |
| 232 | SET_AAA_FLAG | VN, V1 | Sets one of the per-AAA client flags (V1) for the named AAA server (VN):<br>• FLAG_LOG_KEEP_ALIVE<br>• FLAG_LOG_TUNNELS<br>Use the action once for each flag required. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-6 Action Codes for Modifying Network Configuration (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 233 | SET_AAA_TRAFFIC_TYPE | VN, V1 | Sets the appropriate traffic type (V1) for the named AAA server (VN):<br>• TRAFFIC_TYPE_INBOUND<br>• TRAFFIC_TYPE_OUTBOUND<br>• TRAFFIC_TYPE_BOTH<br>The default is TRAFFIC_TYPE_BOTH. |
| 234 | DEL_AAA_SERVER | VN | Deletes the named AAA server (VN). |
| 240 | ADD_PROXY | VN, V1, V2, V3 | Adds a new proxy markup (VN) with markup type (V1) strip markup flag (V2) and accounting flag (V3).<br>The markup type (V1) must be one of the following:<br>• MARKUP_TYPE_PREFIX<br>• MARKUP_TYPE_SUFFIX<br>The markup strip flag should be TRUE if the markup is to be removed from the username before forwarding.<br>The accounting flag (V3) should be one of the following:<br>• ACCT_FLAG_LOCAL<br>• ACCT_FLAG_REMOTE<br>• ACCT_FLAG_BOTH |
| 241 | ADD_PROXY_TARGET | VN, V1 | Adds to named proxy markup (VN) the host name (V1). The host should already be configured on the Cisco Secure ACS.<br>**Note** The order in which proxy targets are added sets the proxy search order; the first target added is the first target proxied to, and so on. The order must be changed through the HTML interface. |
| 242 | DEL_PROXY | VN | Deletes the named proxy markup (VN). |



Downloaded from www.Manualslib.com manuals search engine

*Table F-6 Action Codes for Modifying Network Configuration (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 250 | ADD_NDG | VN | Creates a network device group (NDG) named (VN). |
| 251 | DEL_NDG | VN | Deletes the named NDG. |
| 252 | ADD_HOST_TO_NDG | VN, V1 | Adds to the named AAA client/AAA server (VN) the NDG (V1). |
| 270 | SET_DCS_ ASSIGNMENT | — | — |
| 271 | ADD_NDG_TO_DCS_ MAPPING | — | — |
| 300 | RESTART_PROTO_ MODULES | — | Restarts the CSRadius and CSTacacs services to apply new settings. |
| 350 | ADD_UDV | VN, V1, V2 | Adds a RADIUS vendor to the Cisco Secure ACS vendor database. Vendors added to Cisco Secure ACS by this method are know as User-Defined Vendors (UDV).<br>VN contains the name of the Vendor.<br>**Note** Cisco Secure ACS adds "RADIUS(...)" to the name entered in the Variable Name field. For example, if you enter the name "MyCo", Cisco Secure ACS displays "RADIUS (MyCo)" in the HTML interface.<br>V1 contains the user-defined vendor slot number or AUTO_ASSIGN_SLOT. Cisco Secure ACS has ten vendor slots, numbered 0 through 9. If you specify AUTO_ASSIGN_SLOT, Cisco Secure ACS selects the next available slot for your vendor.<br>**Note** If you want to replicate UDVs between Cisco Secure ACSes, you must assign the UDV to the same slot number on both Cisco Secure ACSes.<br>V2 contains the IANA-assigned enterprise code for the vendor. |



Downloaded from www.Manualslib.com manuals search engine

*Table F-6 Action Codes for Modifying Network Configuration (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 351 | DEL_UDV | V1 | Removes the vendor with the IETF code specified in V1 and any defined VSAs.<br>**Note** Action code 351 does not remove any instances of VSAs assigned to Cisco Secure ACS groups or users. If Cisco Secure ACS has AAA clients configured with the UDV specified in V1, the delete operation fails. |
| 352 | ADD_VSA | VN, V1, V2, V3 | Adds a new VSA to the vendor specified by the vendor IETF code in V1.<br>VN is the VSA name. If the vendor name is MyCo and the attribute is assigned a group ID, we recommend prefixing the vendor name or an abbreviation to all VSAs. For example, VSAs could be "MyCo-Assigned-Group-Id".<br>**Note** VSA names must be unique to both the vendor and to the Cisco Secure ACS dictionary. For example, "MyCo-Framed-IP-Address" is allowed but "Framed-IP-Address" is not, because "Framed-IP-Address" is used by IETF action code 8 in the RADIUS attributes.<br>V2 is the VSA number. This must be in the 0-255 range.<br>V3 is the VSA type as one of following values:<br>• INTEGER<br>• STRING<br>• IPADDR<br>By default, VSAs are assumed to be outbound (or authorization) attributes. If the VSA is either multi-instance or used in accounting messages, use SET_VSA_PROFILE (Action code 353). |



Downloaded from www.Manualslib.com manuals search engine

*Table F-6 Action Codes for Modifying Network Configuration (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 353 | SET_VSA_PROFILE | V1, V2, V3 | Sets the inbound/outbound profile of the VSA. The profile specifies usage "IN" for accounting, "OUT" for authorization, or "MULTI" if more than a singe instance is allowed per RADIUS message. Combinations are allowed.<br>V1 contains the vendor IETF code.<br>V2 contains the VSA number.<br>V3 contains the profile, one of the following:<br>`IN`<br>`OUT`<br>`IN OUT`<br>`MULTI OUT`<br>`MULTI IN OUT` |
| 354 | ADD_VSA_ENUM | VN, V1, V2, V3 | Sets meaningful enumerated values, if the VSA attribute has enumerated. In the User Setup section, the Cisco Secure ACS HTML interface displays the enumeration strings in a list.<br>VN contains the VSA Enum Name.<br>V1 contains the vendor IETF code.<br>V2 contains the VSA number.<br>V3 contains the VSA Enum Value.<br>Example:<br>`VN = Disabled`<br>`V1 = 9034`<br>`V2 = MyCo-Encryption`<br>`V3 = 0`<br>or<br>`VN = Enabled`<br>`V1 = 9034`<br>`V2 = MyCo-Encryption`<br>`V3 = 1` |



Downloaded from www.Manualslib.com manuals search engine

*Table F-6 Action Codes for Modifying Network Configuration (continued)*

| Action Code | Name | Required | Description |
|---|---|---|---|
| 355 | ADOPT_NEW_UDV_ OR_VSA | — | Restarts the CSAdmin, CSRadius, and CSLog services. These services must be restarted before new UDVs or VSAs can become usable. |

# Cisco Secure ACS Attributes and Action Codes

This section complements the previous section by providing an inverse reference; it provides topics with tables that list Cisco Secure ACS attributes, their data types and limits, and the action codes you can use to act upon the Cisco Secure ACS attributes.

This section contains the following topics:


- User-Specific Attributes, page F-32
- User-Defined Attributes, page F-34
- Group-Specific Attributes, page F-35


## User-Specific Attributes

Table F-7 lists the attributes that define a Cisco Secure ACS user, including their data types, limits, and default values. It also provides the action code you can use in accountActions to affect each attribute. Although there are many actions available, adding a user requires only one transaction: ADD_USER. You can safely leave other user attributes at their default values. The term NULL is not simply an empty string, but means not set; that is, the value will not be processed. Some features are processed only if they have a value assigned to them. For more information about action codes, see Action Codes, page F-4.



Downloaded from www.Manualslib.com manuals search engine

*Table F-7 User-Specific Attributes*

| Attribute | Actions | Logical Type | Limits | Default |
|---|---|---|---|---|
| Username | 100, 101 | String | 1-64 characters | — |
| ASCII/PAP Password | 100, 102 | String | 4-32 characters | Random string |
| CHAP Password | 103 | String | 4-32 characters | Random string |
| Outbound CHAP Password | 104 | String | 4-32 characters | NULL |
| TACACS+ Enable Password | 105 | String Password | 4-32 characters | NULL |
| | | Integer privilege level | 0-15 characters | NULL |
| Group | 106 | String | 0-100 characters | "Default Group" |
| Password Supplier | 107 | Enum | See Table F-3. | LIBRARY_CSDB |
| Password Type | 108 | Enum | See Table F-3. | PASS_TYPE_CSDB (password is cleartext PAP) |
| Password Expiry Status | 109, 110 | Bitwise Enum | See Table F-3. | PASS_STATUS_ NEVER (never expires) |
| Expiry Data | 112, 113 | Short wrong max/current | 0-32,767 | — |
| | | Expiry date | — | — |
| Max Sessions | 114 | Unsigned short | 0-65535 | MAX_SESSIONS_AS_GROUP |
| TODDOW Restrictions | 140 | String | 168 characters | 111111111111 |
| NAS Access Control | 120, 122 | Bool enabled | T/F | NULL |
| | | Bool permit/deny | T/F | |
| | | ACL String (See Table F-4.) | 0-31 KB | |



Downloaded from www.Manualslib.com manuals search engine

*Table F-7 User-Specific Attributes (continued)*

| Attribute | Actions | Logical Type | Limits | Default |
|---|---|---|---|---|
| Dial-Up Access Control | 121, 123 | Bool enabled | T/F | NULL |
| | | Bool permit/deny | T/F | NULL |
| | | ACL String (See Table F-4.) | 0-31 KB | NULL |
| Static IP Address | 150 | Enum scheme | (See Table F-4.) | Client |
| | | String IP/Pool name | 0-31 KB | NULL |
| Callback Number | 151 | String | 0-31 KB | NULL |
| TACACS Attributes | 160, 162 | Formatted String | 0-31 KB | NULL |
| RADIUS Attributes | 170, 173 | Formatted String | 0-31 KB | NULL |
| UDF 1 | 1, 2 | String Real Name | 0-31 KB | NULL |
| UDF 2 | 1, 2 | String Description | 0-31 KB | NULL |
| UDF 3 | 1, 2 | String | 0-31 KB | NULL |
| UDF 4 | 1, 2 | String | 0-31 KB | NULL |
| UDF 5 | 1, 2 | String | 0-31 KB | NULL |

# User-Defined Attributes

User-defined attributes (UDAs) are string values that can contain any data, such as social security number, department name, telephone number, and so on. You can configure Cisco Secure ACS to include UDAs on accounting logs about user activity. For more information about configuring UDAs, see User Data Configuration Options, page 3-3.



Downloaded from www.Manualslib.com manuals search engine

RDBMS Synchronization can set UDAs by using the SET_VALUE action (code 1) to create a value called “USER_DEFINED_FIELD_0” or “USER_DEFINED_FIELD_1”. For accountActions rows defining a UDA value, the AppId (AI) field must contain “APP_ CSAUTH” and the Value2(V2) field must contain “TYPE_STRING”.

Table F-8 lists the data fields that define UDAs. For more information about action codes, see Action Codes, page F-4.

***Table F-8 User-Defined Attributes***

| Action | Username (UN) | ValueName (VN) | Value1 (V1) | Value2 (V2) | AppId (AI) |
|---|---|---|---|---|---|
| 1 | fred | USER_DEFINED_ FIELD_0 | SS123456789 | TYPE_STRING | APP_CSAUTH |
| 1 | fred | USER_DEFINED_ FIELD_1 | Engineering | TYPE_STRING | APP_CSAUTH |
| 1 | fred | USER_DEFINED_ FIELD_2 | 949-555-1111 | TYPE_STRING | APP_CSAUTH |

**Note** If more than two UDAs are created, only the first two are passed to accounting logs.

# Group-Specific Attributes

Table F-9 lists the attributes that define a Cisco Secure ACS group, including their data types, limits, and default values. It also provides the action code you can use in your accountActions table to affect each field. For more information about action codes, see Action Codes, page F-4.



Downloaded from www.Manualslib.com manuals search engine

*Table F-9 Group-Specific Attributes*

| Attribute | Actions | Logical Type | Limits | Default |
|---|---|---|---|---|
| Max Sessions | 114 | Unsigned short | 0-65534 | MAX_SESSIONS_ UNLIMITED |
| Max Sessions for user of group | 115 | Unsigned short | 0-65534 | MAX_SESSIONS_ UNLIMITED |
| Token caching for session | 130 | Bool | T/F | NULL |
| Token caching for duration | 131 | Integer time in seconds | 0-65535 | NULL |
| TODDOW Restrictions | 140 | String | 168 characters | 111111111111 |
| NAS Access Control | 120, 122 | Bool enabled | T/F | NULL |
| | | Bool permit/deny | T/F | |
| | | ACL String (See Table F-4.) | 0-31 KB | |
| Dial-Up Access Control | 121, 123 | Bool enabled | T/F | NULL |
| | | Bool permit/deny | T/F | NULL |
| | | ACL String (See Table F-4.) | 0-31 KB | NULL |
| Static IP Address | 150 | Enum scheme | (See Table F-4.) | Client |
| | | String IP/Pool name | 0-31 KB | NULL |
| TACACS Attributes | 160, 162 | Formatted String | 0-31 KB | NULL |
| RADIUS Attributes | 170, 173 | Formatted String | 0-31 KB | NULL |
| VoIP Support | 212 | Bool disabled | T/F | NULL |

# An Example of accountActions

Table F-10 presents an sample instance of accountActions that contains some of the action codes described in Action Codes, page F-4. First user “fred” is created, along with his passwords, including a TACACS_ Enable password with privilege



Downloaded from www.Manualslib.com manuals search engine

level 10. Fred is assigned to "Group 2". His account expires after December 31, 1999, or after 10 incorrect authentication attempts. Attributes for Group 2 include Time-of-Day/Day-of-Week restrictions, token caching, and some RADIUS attributes.

**Note** This example omits several columns that should appear in any accountActions table. The omitted columns are Sequence ID (SI), Priority (P), DateTime (DT), and MessageNo (MN).

*Table F-10 Example accountActions Table*

| Action | User name (UN) | Group Name (GN) | Value Name (VN) | Value1 (V1) | Value2 (V2) | Value3 (V3) | AppId (AI) |
|---|---|---|---|---|---|---|---|
| 100 | fred | — | — | fred | — | — | — |
| 102 | fred | — | — | freds_password | — | — | — |
| 103 | fred | — | — | freds_chap_ password | — | — | — |
| 104 | fred | — | — | freds_outbound_ password | — | — | — |
| 105 | fred | — | — | freds_enable_ password | 10 | — | — |
| 106 | fred | Group 2 | — | — | — | — | — |
| 150 | fred | — | — | 123.123.123.123 | — | — | — |
| 151 | fred | — | — | 01832-123900 | — | — | — |
| 109 | fred | — | — | PASS_STATUS_ NEVER | — | — | — |
| 110 | fred | — | — | PASS_STATUS_ WRONG | — | — | — |
| 110 | fred | — | — | PASS_STATUS_ EXPIRES | — | — | — |
| 112 | fred | — | — | 10 | — | — | — |
| 113 | fred | — | — | 19991231 | — | — | — |



Downloaded from www.Manualslib.com manuals search engine

*Table F-10 Example accountActions Table (continued)*

| Action | User name (UN) | Group Name (GN) | Value Name (VN) | Value1 (V1) | Value2 (V2) | Value3 (V3) | AppId (AI) |
|---|---|---|---|---|---|---|---|
| 114 | fred | — | — | 50 | — | — | — |
| 115 | fred | — | — | 50 | — | — | — |
| 120 | fred | — | — | ACCESS_PERMIT | — | — | — |
| 121 | fred | — | — | ACCESS_DENY | — | — | — |
| 122 | fred | — | — | NAS01,tty0,01732-975374 | — | — | — |
| 123 | fred | — | — | 01732-975374,01622-123123 | CLID/ DNIS | — | — |
| 1 | fred | — | USER_ DEFINED_ FIELD_0 | Fred Jones | TYPE_ STRING | — | APP_ CSAUTH |
| 140 | — | Group 2 | — | [a string of 168 ones (1)] | — | — | — |
| 130 | — | Group 2 | — | DISABLE | — | — | — |
| 131 | — | Group 2 | — | 61 | — | — | — |
| 163 | — | Group 2 | Reply-Message | Welcome to Your Internet Service | — | — | — |
| 163 | — | Group 2 | Vendor-Specific | addr-pool=pool2 | 9 | 1 | — |



Downloaded from www.Manualslib.com manuals search engine

# Internal Architecture

This chapter describes the Cisco Secure ACS for Windows Server architectural components. It includes the following topics:


- Windows Services, page G-1
- Windows Registry, page G-2
- CSAdmin, page G-2
- CSAuth, page G-3
- CSDBSync, page G-4
- CSLog, page G-4
- CSMon, page G-4
- CSTacacs and CSRadius, page G-8


## Windows Services

Cisco Secure ACS is modular and flexible to fit the needs of both simple and large networks. This appendix describes the Cisco Secure ACS architectural components. Cisco Secure ACS includes the following service modules:

- CSAdmin
- CSAuth
- CSDBSync
- CSLog



Downloaded from www.Manualslib.com manuals search engine

- CSMon
- CSTacacs
- CSRadius

You can stop or restart Cisco Secure ACS services as a group, except for CSAdmin, using the Cisco Secure ACS HTML interface. For more information, see Service Control, page 8-1.

Individual Cisco Secure ACS services can be started, stopped, and restarted from the Services window, available within Windows Control Panel.

# Windows Registry

The Cisco Secure ACS information is located in the following Windows Registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\CISCO
```

Unless you are advised to do so by a Cisco representative, we strongly recommend that you do not modify Windows Registry settings pertaining to Cisco Secure ACS.

**Warning** **Do not modify the Registry unless you have enough knowledge and experience to edit the file without destroying or corrupting crucial data.**

# CSAdmin

CSAdmin is the service that provides the web server for the Cisco Secure ACS HTML interface. After Cisco Secure ACS is installed, you must configure it from its HTML interface; therefore, CSAdmin must be running when you configure Cisco Secure ACS.

Because the Cisco Secure ACS web server uses port 2002 rather than the standard port 80 usually associated with HTTP traffic, you can use another web server on the same machine to provide other web services. We have not performed interoperability testing with other web servers, but unless a second web server is configured to use either port 2002 or one of the ports within the range specified



Downloaded from www.Manualslib.com manuals search engine

in the HTTP Port Allocation feature, you should not encounter port conflicts for HTTP traffic. For more information about the HTTP Port Allocation feature, see Access Policy, page 12-11.

**Note** For more information about access to the HTML interface and network environments, see Network Environments and Administrative Sessions, page 1-30.

Although you can start and stop services from within the Cisco Secure ACS HTML interface, this does not include starting or stopping CSAdmin. If CSAdmin stops abnormally because of an external action, you cannot access Cisco Secure ACS from any computer other than the Windows server on which it is running. You can start or stop CSAdmin from Windows Control Panel.

CSAdmin is multi-threaded, which enables several Cisco Secure ACS administrators to access it at the same time. Therefore, CSAdmin is well suited for distributed, multiprocessor environments.

# CSAuth

CSAuth is the authentication and authorization service. It permits or denies access to users by processing authentication and authorization requests. CSAuth determines if access should be granted and defines the privileges for a particular user. CSAuth is the Cisco Secure ACS database manager.

To authenticate users, Cisco Secure ACS can use the internal user database or one of many external databases. When a request for authentication arrives, Cisco Secure ACS checks the database that is configured for that user. If the user is unknown, Cisco Secure ACS checks the database(s) configured for unknown users. For more information about how Cisco Secure ACS handles authentication requests for unknown users, see About Unknown User Authentication, page 15-4.

For more information about the various database types supported by Cisco Secure ACS, see Chapter 13, “User Databases”.

When a user has authenticated, Cisco Secure ACS obtains a set of authorizations from the user profile and the group to which the user is assigned. This information is stored with the username in the CiscoSecure user database. Some of the authorizations included are the services to which the user is entitled, such as IP over PPP, IP pools from which to draw an IP address, access lists, and



Downloaded from www.Manualslib.com manuals search engine

password-aging information. The authorizations, with the approval of authentication, are then passed to the CSTacacs or CSRadius modules to be forwarded to the requesting device.

# CSDBSync

CSDBSync is the service used to synchronize the Cisco Secure ACS database with third-party relational database management system (RDBMS) systems. CSDBSync synchronizes AAA client, AAA server, network device groups (NDGs) and Proxy Table information with data from a table in an external relational database. For information on RDBMS Synchronization, see RDBMS Synchronization, page 9-25.

# CSLog

CSLog is the service used to capture and place logging information. CSLog gathers data from the TACACS+ or RADIUS packet and CSAuth, and then manipulates the data to be placed into the comma-separated value (CSV) files. CSV files can be imported into spreadsheets that support this format.

For information about the logs generated by Cisco Secure ACS, see Chapter 1, “Overview”.

# CSMon

CSMon is a service that helps minimize downtime in a remote access network environment. CSMon works for both TACACS+ and RADIUS and automatically detects which protocols are in use.

You can use the Cisco Secure ACS HTML interface to configure the CSMon service. The Cisco Secure ACS Active Service Management feature provides options for configuring CSMon behavior. For more information, see Cisco Secure ACS Active Service Management, page 8-17.



Downloaded from www.Manualslib.com manuals search engine

**Note** CSMon is not intended as a replacement for system, network, or application management applications but is provided as an application-specific utility that can be used with other, more generic system management tools.

CSMon performs four basic activities, outlined in the following topics:


- Monitoring, page G-5
- Recording, page G-6
- Notification, page G-7
- Response, page G-7


# Monitoring

CSMon monitors the overall status of Cisco Secure ACS and the system on which it is running. CSMon actively monitors three basic sets of system parameters:

- **Generic host system state**—CSMon monitors the following key system thresholds:
  - Available hard disk space
  - Processor utilization
  - Physical memory utilization

  All events related to generic host system state are categorized as "warning events".
- **Application-specific performance**
  - **Application viability**—CSMon periodically performs a test login using a special built-in test account (the default period is one minute). Problems with this authentication can be used to determine if the service has been compromised.
  - **Application performance thresholds**—CSMon monitors and records the latency of each test authentication request (the time it takes to receive a positive response). Each time this is performed, CSMon updates a variable containing the average response time value. Additionally, it records whether retries were necessary to achieve a successful response. By tracking the average time for each test authentication, CSMon can



Downloaded from www.Manualslib.com manuals search engine

build up a "picture" of expected response time on the system in question. CSMon can therefore detect whether excess re-tries are required for each authentication or if response times for a single authentication exceed a percentage threshold over the average.

- **System resource consumption by Cisco Secure ACS**—CSMon periodically monitors and records the usage by Cisco Secure ACS of a small set of key system resources and compares it against predetermined thresholds for indications of atypical behavior. The parameters monitored include the following:
  - Handle counts
  - Memory utilization
  - Processor utilization
  - Thread used
  - Failed log-on attempts

CSMon cooperates with CSAuth to keep track of user accounts being disabled by exceeding their failed attempts count maximum. This feature is more oriented to security and user support than to system viability. If configured, it provides immediate warning of "brute force" attacks by alerting the administrator to a large number of accounts becoming disabled. In addition, it helps support technicians anticipate problems with individual users gaining access.

# Recording

CSMon records exception events in logs that you can use to diagnose problems.

- **CSMon Log**—Like the other Cisco Secure ACS services, CSMon maintains a CSV log of its own for diagnostic recording and error logging. Because this logging consumes relatively small amounts of resources, CSMon logging cannot be disabled.
- **Windows Event Log**—CSMon can log messages to the Windows Event Log. Logging to the Windows Event Log is enabled by default but can be disabled.



Downloaded from www.Manualslib.com manuals search engine

# Notification

CSMon can be configured to notify system administrators in the following cases:

- Exception events
- Response
- Outcome of the response

Notification for exception events and outcomes includes the current state of Cisco Secure ACS at the time of the message. The default notification method is simple mail-transfer protocol (SMTP) e-mail, but you can create scripts to enable other methods.

# Response

CSMon detects exception events that affect the integrity of the service. For information about monitored events, see Monitoring, page G-5. These events are application-specific and hard-coded into Cisco Secure ACS. There are two types of responses:

- **Warning events**—Service is maintained but some monitored threshold is breached.
- **Failure events**—One or more Cisco Secure ACS components stop providing service.

CSMon responds to the event by logging the event, sending notifications (if configured) and, if the event is a failure, taking action. There are two types of actions:

- **Predefined actions**—These actions are hard-coded into the program and are always carried out when a triggering event is detected. Because these actions are hard-coded, they are integral to the application and do not need to be configured. These actions include running the CSSupport utility, which captures most of the parameters dealing with the state of the system at the time of the event.



Downloaded from www.Manualslib.com manuals search engine

If the event is a warning event, it is logged and the administrator is notified. No further action is taken. CSMon also attempts to fix the cause of the failure after a sequence of re-tries and individual service restarts.

- **Customer-Definable Actions**—If the predefined actions built into CSMon do not fix the problem, CSMon can execute an external program or script.

# CSTacacs and CSRadius

The CSTacacs and CSRadius services communicate between the CSAuth module and the access device that is requesting authentication and authorization services. For CSTacacs and CSRadius to work properly, the system must meet the following conditions:

- CSTacacs and CSRadius services must be configured from CSAdmin.
- CSTacacs and CSRadius services must communicate with access devices such as access servers, routers, switches, and firewalls.
- The identical shared secret (key) must be configured both in Cisco Secure ACS and on the access device.
- The access device IP address must be specified in Cisco Secure ACS.
- The type of security protocol being used must be specified in Cisco Secure ACS.

CSTacacs is used to communicate with TACACS+ devices and CSRadius to communicate with RADIUS devices. Both services can run at the same time. When only one security protocol is used, only the applicable service needs to be running; however, the other service will not interfere with normal operation and does not need to be disabled. For more information about TACACS+ AV pairs, see Appendix B, “TACACS+ Attribute-Value Pairs”. For more information about RADIUS+ AV pairs, see Appendix C, “RADIUS Attributes”.



Downloaded from www.Manualslib.com manuals search engine

# A


AAA
- See also AAA clients
- See also AAA servers
- definition 1-2
- pools for IP address assignment 7-11

AAA clients
- adding and configuring 4-16
- configuration 4-11
- definition 1-6
- deleting 4-21
- editing 4-19
- interaction with AAA servers 1-6
- IP pools 7-11
- multiple IP addresses for 4-12
- number of 1-4
- searching for 4-8
- supported Cisco AAA clients 1-2
- table 4-1
- timeout values 15-9

AAA servers
- adding 4-24
- configuring 4-21
- deleting 4-28
- editing 4-26
- enabling in interface (table) 3-5
- functions and concepts 1-5
- in distributed systems 4-3
- master 9-3
- overview 4-21
- primary 9-3
- replicating 9-3
- searching for 4-8
- secondary 9-3
- troubleshooting A-1

access devices 1-6

accessing Cisco Secure ACS
- how to 1-32
- URL 1-29
- with SSL enabled 1-29

access policies
- See administrative access policies

accountActions table 9-29, 9-31

account disablement
- Account Disabled check box 7-5
- manual 7-56
- resetting 7-59
- setting options for 7-20





Downloaded from www.Manualslib.com manuals search engine

accounting
See also logging
overview 1-22
ACLs
See downloadable IP ACLs
action codes
for creating and modifying user accounts F-7
for initializing and modifying access filters F-14
for modifying network configuration F-25
for modifying TACACS+ and RADIUS settings F-19
for setting and deleting values F-5
in accountActions F-4
Active Service Management
See Cisco Secure ACS Active Service Management
Administration Audit log
configuring 11-14
CSV file directory 11-16
viewing 11-18
Administration Control
See also administrators
audit policy setup 12-18
administrative access policies
See also administrators
configuring 12-14
limits 12-11
options 12-12
overview 2-15
administrative sessions
and HTTP proxy 1-30
network environment limitations of 1-30
session policies 12-16
through firewalls 1-31
through NAT (network address translation) 1-31
administrators
See also Administration Audit log
See also Administration Control
See also administrative access policies
adding 12-6
deleting 12-11
editing 12-7
locked out 12-10
locking out 12-17
overview 12-2
privileges 12-3
separation from general users 2-17
troubleshooting A-2
unlocking 12-10
advanced options in interface 3-6
age-by-date rules for groups 6-25
Aironet
AAA client configuration 4-13
RADIUS parameters for group 6-41
RADIUS parameters for user 7-41
ARAP
compatible databases 1-10
in User Setup 7-5



Downloaded from www.Manualslib.com manuals search engine

protocol supported 1-11
Architecture G-1
ASCII/PAP
compatible databases 1-10
protocol supported 1-11
attributes
enabling in interface 3-2
group-specific (table) F-35
logging of user data 11-2
per-group 3-2
per-user 3-2
user-specific (table) F-34
attribute-value pairs
See AV (attribute value) pairs
audit policies
See also Administration Audit log
overview 12-18
authentication
compatibility of protocols 1-10
configuration 10-26
denying unknown users 15-17
options 10-33
overview 1-8
request handling 15-5
via external user databases 13-5
Windows 13-11
authorization 1-17
authorization sets
See command authorization sets
AV (attribute value) pairs
See also RADIUS VSAs (vendor specific attributes)
RADIUS
Cisco IOS C-3
IETF C-14
TACACS+
accounting B-4
general B-1

## B

Backup and Restore log directory
See Cisco Secure ACS Backup and Restore log
backups
components backed up 8-10
directory management 8-10
disabling scheduled 8-13
filenames 8-15
locations 8-10
manual 8-12
options 8-11
overview 8-9
reports 8-11
scheduled vs. manual 8-9
scheduling 8-12
vs. replication 9-10
with CSUtil.exe D-6



Downloaded from www.Manualslib.com manuals search engine

browsers
See also HTML interface
troubleshooting A-4

## C

cached users
See discovered users
CA configuration 10-38
callback options
in Group Setup 6-7
in User Setup 7-9
cascading replication 9-6, 9-13
cautions
significance of xxxii
certification
See also EAP-TLS
See also PEAP
adding certificate authority certificates 10-37
background 10-1
backups 8-10
Certificate Revocation Lists 10-40
certificate signing request generation 10-45
editing the certificate trust list 10-38
replacing certificate 10-50
self-signed certificates
configuring 10-49
NAC 14-6
overview 10-47
server certificate installation 10-35
updating certificate 10-50
CHAP
compatible databases 1-10
in User Setup 7-5
protocol supported 1-11
Cisco IOS
RADIUS
AV (attribute value) pairs C-2
group attributes 6-40
user attributes 7-39
TACACS+ AV (attribute value) pairs B-1
troubleshooting A-5
Cisco Secure ACS Active Service Management
event logging configuration 8-20
overview 8-17
system monitoring
configuring 8-19
custom actions 8-18
Cisco Secure ACS Active Service Monitoring logs
file location 11-17
viewing 11-18
Cisco Secure ACS administration overview 1-23
Cisco Secure ACS Backup and Restore log
CSV (comma-separated values) file directory 11-16
viewing 11-18



Downloaded from www.Manualslib.com manuals search engine

Cisco Secure ACS backups
See backups
Cisco Secure ACS system restore
See restore
CiscoSecure Authentication Agent 1-16, 6-21
CiscoSecure database replication
See replication
CiscoSecure user database
See also databases
overview 13-2
password encryption 13-2
Cisco Trust Agent
definition 14-2
unavailable 14-5
CLID-based filters 5-18
codes
See action codes
command authorization sets
See also shell command authorization sets
adding 5-31
configuring 5-25, 5-31
deleting 5-35
editing 5-33
overview 5-26
pattern matching 5-30
PIX command authorization sets 5-26
command-line database utility
See CSUtil.exe
conventions xxxi
CRLs 10-40
CSAdmin G-2
CSAuth G-3
CSDBSync 9-29, G-4
CSLog G-4
CSMon
See also Cisco Secure ACS Active Service Management
Cisco Secure ACS Service Monitoring logs 11-32
configuration G-4
failure events
customer-defined actions G-7
predefined actions G-7
functions G-4
log G-6
overview G-4
CSNTacctInfo 13-65, 13-67, 13-68
CSNTAuthUserPap 13-62
CSNTerrorString 13-65, 13-67, 13-68
CSNTExtractUserClearTextPw 13-63
CSNTFindUser 13-64
CSNTgroups 13-65, 13-67, 13-68
CSNTpasswords 13-65, 13-67
CSNTresults 13-65, 13-67, 13-68
CSNTusernames 13-65, 13-66, 13-68
CSRadius G-8
CSTacacs G-8
CSUtil.exe
decoding error numbers with D-27



Downloaded from www.Manualslib.com manuals search engine

displaying syntax D-5
import text file (example) D-24
overview D-1
CSV (comma-separated values) files
downloading 11-18
filename formats 11-15
logging format 11-2
viewing 11-18
CTL editing 10-38
custom attributes
in group-level TACACS+ settings 6-31
in user-level TACACS+ settings 7-23

## D

database group mappings
configuring
for token servers 16-3
for Windows domains 16-9
no access groups 16-7
order 16-12
deleting
group set mappings 16-10
Windows domain configurations 16-11
in external user databases 16-1
overview 16-1
Database Replication log
CSV (comma-separated values) file directory 11-16
viewing 11-18
databases
See also external user databases
authentication search process 15-5
CiscoSecure user database 13-2
compacting D-12
deleting 13-86
deployment considerations 2-18
dump files D-10
external
See also external user databases
See also Unknown User Policy
NAC 14-10
posture validation search process 15-11
protocol compatibility 1-10
replication
See replication
search order 15-14
search process 15-14
selecting user databases 13-1
synchronization
See RDBMS synchronization
token cards
See token servers
troubleshooting A-7, A-19
types
See generic LDAP user databases
See LEAP proxy RADIUS user databases
See Novell NDS user databases
See ODBC features



Downloaded from www.Manualslib.com manuals search engine

See RADIUS user databases
See RSA user databases
unknown users 15-1
user databases 7-2
user import methods 13-3
Windows user databases 13-7
data source names
configuring for ODBC logging 11-22
for RDMBS synchronization 9-38
using with ODBC databases 13-56, 13-70, 13-72
date format control 8-3
DbSync log directory 11-16
debug logs
detail levels 11-33
frequency 11-33
troubleshooting A-14
default group in Group Setup 6-2
default group mapping for Windows 16-6
default time-of-day/day-of-week specification 3-5
default time-of-day access settings for groups 6-5
deleting logged-in users 11-11
deployment
overview 2-1
sequence 2-19
device command sets
See command authorization sets
device groups
See network device groups
device management applications support 1-19
DHCP with IP pools 9-45
dial-in permission to users in Windows 13-26
dial-in troubleshooting A-10
dial-up networking clients 13-10
dial-up topologies 2-6
digital certificates
See certification
Disabled Accounts report
viewing 11-12
Disabled Accounts reports
description 11-9
discovered users 15-3
distributed systems
See also proxy
AAA servers in 4-3
overview 4-2
settings
configuring 4-34
default entry 4-3
enabling in interface 3-5
distribution table
See Proxy Distribution Table
DNIS-based filters 5-18
documentation
conventions xxxi
objectives xxix
online 1-33
related xxxiii




Downloaded from www.Manualslib.com manuals search engine

Domain List
configuring 13-30
inadvertent user lockouts 13-14, 13-27
overview 13-13
unknown user authentication 15-7
domain names
Windows operating systems 13-13, 13-14
downloadable IP ACLs
adding 5-10
assigning to groups 6-30
assigning to users 7-21
deleting 5-14
editing 5-13
enabling in interface
group-level 3-5
user-level 3-5
overview 5-7
draft-ietf-radius-tunnel-auth 1-7
dump files
creating database dump files D-10
loading a database from a dump file D-11

## E

EAP (Extensible Authentication Protocol)
overview 1-13
with Windows authentication 13-15
EAP-FAST
compatible databases 1-10
enabling 10-25
identity protection 10-14
logging 10-14
master keys
definition 10-15
states 10-15
master server 10-23
options 10-28
overview 10-13
PAC
automatic provisioning 10-18
definition 10-17
manual provisioning 10-20
refresh 10-21
states 10-18
password aging 6-27
phases 10-13
replication 10-22
EAP-TLS
See also certification
authentication configuration 10-26
comparison methods 10-4
compatible databases 1-10
domain stripping 13-16
enabling 10-7
limitations 10-6
options 10-31
overview 10-3
session resume 10-5



Downloaded from www.Manualslib.com manuals search engine

enable password options for TACACS+ 7-35
enable privilege options for groups 6-19
error number decoding with CSUtil.exe D-27
Event log
  configuring 8-20
  exception events G-6
exception events G-7
exports
  of user lists D-24
Extensible Authentication Protocol
  See EAP (Extensible Authentication Protocol)
external token servers
  See token servers
external user databases
  See also databases
  authentication via 13-5
  configuring 13-4
  deleting configuration 13-86
  latency factors 15-9
  search order 15-9, 15-15
  supported 1-10
  Unknown User Policy 15-1

## F

Failed Attempts log
  configuring
    CSV (comma-separated values) 11-19
    ODBC 11-23
    CSV (comma-separated values) file directory 11-16
  enabling
    log 11-17
    ODBC 11-23
  viewing 11-18
failed log-on attempts G-6
failure events
  customer-defined actions G-7
  predefined actions G-7
fallbacks on failed connection 4-5
finding users 7-55
firewalls
  administering AAA servers through 1-23

## G

gateways E-3
generic LDAP user databases
  authentication 13-32
  configuring
    database 13-43
    options 13-37
  directed authentications 13-34
  domain filtering 13-34
  failover 13-36
  mapping database groups to AAA groups 16-4
  multiple instances 13-33
  organizational units and groups 13-34



Downloaded from www.Manualslib.com manuals search engine

supported protocols 1-10
Global Authentication Setup 10-33
grant dial-in permission to users 13-9, 13-26
greeting after login 6-24
group-level interface enabling
downloadable IP ACLs 3-5
network access restrictions 3-5
network access restriction sets 3-5
password aging 3-5
group-level network access restrictions
See network access restrictions
groups
See also network device groups
assigning users to 7-8
configuring RADIUS settings for
See RADIUS
Default Group 6-2, 16-6
enabling VoIP (Voice-over-IP) support for 6-4
exporting group information D-25
listing all users in 6-54
mapping order 16-12
mappings 16-1, 16-2
multiple mappings 16-5
no access groups 16-5
overriding settings 3-2
relationship to users 3-2
renaming 6-55
resetting usage quota counters for 6-55
settings for
callback options 6-7
configuration-specific 6-16
configuring common 6-3
device management command authorization sets 6-37
enable privilege 6-19
IP address assignment method 6-28
management tasks 6-54
max sessions 6-12
network access restrictions 6-8
password aging rules 6-21
PIX command authorization sets 6-35
shell command authorization sets 6-33
TACACS+ 6-2, 6-31
time-of-day access 6-5
token cards 6-18
usage quotas 6-14
setting up and managing 6-1
sort order within group mappings 16-5
specifications by ODBC authentications 13-65, 13-67, 13-68
GUI
See HTML interface


## H


handle counts G-6
hard disk space G-5
hardware requirements 2-2




Downloaded from www.Manualslib.com manuals search engine

Help 1-29
host system state G-5
HTML interface
See also Interface Configuration
encrypting 12-13
logging off 1-33
overview 1-25
security 1-26
SSL 1-26
web servers G-2
HTTP port allocation
configuring 12-14
overview 1-23
HTTPS 12-13

## I

IETF 802.1x 1-13
importing passwords D-14
imports with CSUtil.exe D-14
inbound authentication 1-14
inbound password configuration 1-14
installation
related documentation xxxiii
system requirements 2-2
troubleshooting A-16
Interface Configuration
See also HTML interface
advanced options 3-4
configuring 3-1
customized user data fields 3-3
security protocol options 3-9
IP ACLs
See downloadable IP ACLs
IP addresses
in User Setup 7-10
multiple IP addresses for AAA client 4-12
requirement for CSTacacs and CSRadius G-8
setting assignment method for user groups 6-28
IP pools
address recovery 9-51
deleting 9-50
DHCP 9-45
editing IP pool definitions 9-48
enabling in interface 3-6
overlapping 9-45, 9-47
refreshing 9-47
resetting 9-49
servers
adding IP pools 9-47
overview 9-44
replicating IP pools 9-45
user IP addresses 7-11

## L

LAN manager 1-13
latency in networks 2-19



Downloaded from www.Manualslib.com manuals search engine

LDAP
See generic LDAP user databases
LEAP proxy RADIUS user databases
configuring external databases 13-76
group mappings 16-2
overview 13-75
RADIUS-based group specifications 16-14
list all users
in Group Setup 6-54
in User Setup 7-55
Logged-In Users report
deleting logged-in users 11-11
description 11-10
viewing 11-10
logging
See also Reports and Activity
accounting logs 11-6
Administration Audit log 11-14
administration reports 11-9
configuring 11-20
CSV (comma-separated values) files 11-2
custom RADIUS dictionaries 9-2
debug logs
detail levels 11-33
frequency 11-33
Disabled Accounts reports 11-9
domain names 11-3
external user databases 11-3
Failed Attempts logs 11-6
formats 11-2
Logged-In Users reports 11-9
ODBC logs
enabling in interface 3-6
overview 11-2
working with 11-21
overview 11-6
Passed Authentication logs 11-6
RADIUS logs 11-6
RDBMS synchronization 9-2
remote logging
centralized 11-27
configuring 11-29
disabling 11-31
enabling in interface 3-5
logging hosts 11-26
options 11-28
overview 11-26
services
configuring service logs 11-33
list of logs generated 11-32
system logs 11-13
TACACS+ logs 11-6
troubleshooting A-17
user data attributes 11-2
VoIP logs 11-6
watchdog packets 11-5
login process test frequency 8-18



Downloaded from www.Manualslib.com manuals search engine

logins
greeting upon 6-24
password aging dependency 6-23
logs
See logging
See Reports and Activity

## M

machine authentication
enabling 13-22
overview 13-16
with Microsoft Windows 13-20
management application support 1-19
mappings
database groups to AAA groups 16-4
databases to AAA groups 16-2
master AAA servers 9-3
master key
definition 10-15
states 10-15
max sessions
enabling in interface 3-5
in Group Setup 6-12
in User Setup 7-16
overview 1-18
troubleshooting A-16
memory utilization G-5
monitoring
configuring 8-19
CSMon G-5
overview 8-18
MS-CHAP
compatible databases 1-10
configuring 10-26
overview 1-13
protocol supported 1-11
multiple group mappings 16-5
multiple IP addresses for AAA clients 4-12

## N

NAC
attributes
about 14-11
adding D-44
data types 14-19
deleting D-44
exporting D-44
attribute-value pairs 14-9
Certificate Trust List 14-6
credentials
about 14-11
definition 14-2
databases
configuring 14-14
default database 14-10



Downloaded from www.Manualslib.com manuals search engine

definition of 14-10
group mapping 16-13
implementing 14-5
introduction 1-25
logging 14-6
NAC client
Cisco Trust Agent 14-2
definition 14-2
policies
about 14-16
external 14-28
local 14-17
results 14-16
remediation server
definition 14-2
url-redirect attribute C-8
rules
about 14-19
default 14-23
operators 14-20
self-signed certificates 14-6
tokens
assigning to rules 14-23
definition 14-4
group mapping 16-13
returned by local policies 14-18
Unknown User Policy 15-10
NAFs
See network access filters
NAR
See network access restrictions
NAS
See AAA clients
NDG
See network device groups
NDS
See Novell NDS user databases
network access filters
adding 5-3
deleting 5-7
editing 5-5
overview 5-2
network access quotas 1-18
network access restrictions
adding 5-19
configuring 5-19
deleting 5-24
editing 5-23
enabling in interface
group-level 3-5
user-level 3-5
in Group Setup 6-8
interface configuration 3-5
in User Setup 6-8, 7-11
non-IP-based filters 5-18
overview 5-15
network access servers
See AAA clients




Downloaded from www.Manualslib.com manuals search engine

Network Admission Control
See NAC
network configuration 4-1
network device groups
adding 4-29
assigning AAA clients to 4-30
assigning AAA servers to 4-30
configuring 4-28
deleting 4-32
enabling in interface 3-6
overview 1-24
reassigning AAA clients to 4-31
reassigning AAA servers to 4-31
renaming 4-32
network devices
See AAA clients
searches for 4-8
network requirements 2-4
networks
latency 2-19
reliability 2-19
network topologies
deployment 2-6
wireless 2-9
notifications G-7
Novell NDS user databases
authentication 13-50
configuring 13-53
mapping database groups to AAA groups 16-4
Novell Requestor 13-50
options 13-52
supported protocols 1-10
supported versions 13-50
user contexts 13-51

## O

ODBC features
accountActions table 9-32
authentication
CHAP 13-60
EAP-TLS 13-60
overview 13-55
PAP 13-60
preparation process 13-59
process with external user database 13-58
result codes 13-69
case-sensitive passwords 13-61
CHAP authentication sample procedure 13-63
configuring 13-71
data source names 11-22, 13-56
DSN (data source name) configuration 13-70
EAP-TLS authentication sample procedure 13-64
features supported 13-57
group mappings 16-2
group specifications
CHAP 13-67



Downloaded from www.Manualslib.com manuals search engine

EAP-TLS 13-68
PAP 13-65
vs. group mappings 16-3
PAP authentication sample procedures 13-62
password case sensitivity 13-61
stored procedures
CHAP authentication 13-66
EAP-TLS authentication 13-67
implementing 13-60
PAP authentication 13-64
type definitions 13-61
user databases 13-55
ODBC logs
See logging
Online Documentation 1-34
online Help
location in HTML interface 1-29
using 1-34
operating system requirements 2-2
outbound password configuration 1-15
overview of Cisco Secure ACS 1-1


## P


PAC
automatic provisioning 10-18
definition 10-17
manual provisioning 10-20
refresh 10-21
PAP
compatible databases 1-10
in User Setup 7-5
vs. ARAP 1-12
vs. CHAP 1-12
Passed Authentications log
configuring CSV (comma-separated values) 11-19
CSV (comma-separated values) file directory 11-16
enabling CSV (comma-separated values) logging 11-17
viewing 11-18
password aging
age-by-uses rules 6-23
Cisco IOS release requirement for 6-21
EAP-FAST 13-25
interface configuration 3-5
in Windows databases 6-26
MS-CHAP 13-25
overview 1-15
PEAP 13-25
rules 6-21
passwords
See also password aging
case sensitive 13-61
CHAP/MS-CHAP/ARAP 7-7
configurations
caching 1-15
inbound passwords 1-14




Downloaded from www.Manualslib.com manuals search engine

outbound passwords 1-15
separate passwords 1-14
single password 1-14
token caching 1-15
token cards 1-14
encryption 13-2
expiration 6-23
import utility D-14
local management 8-5
password change log management 8-6
post-login greeting 6-24
protocols and user database compatibility 1-10
protocols supported 1-11
remote change 8-5
user-changeable 1-16
validation options in System Configuration 8-5
pattern matching in command authorization 5-30
PEAP
See also certification
compatible databases 1-10
configuring 10-26
enabling 10-12
identity protection 10-9
options 10-27
overview 10-8
password aging 6-27
phases 10-9
with Unknown User Policy 10-11
performance monitoring G-5
performance specifications 1-3
per-group attributes
See also groups
enabling in interface 3-2
per-user attributes
enabling in interface 3-2
TACACS+/RADIUS in Interface Configuration 3-4
PIX ACLs
See downloadable IP ACLs
PIX command authorization sets
See command authorization sets
PKI (public key infrastructure)
See certification
port 2002
CSAdmin G-2
in HTTP port ranges 12-13
in URLs 1-29
port allocation
See HTTP port allocation
ports
See also HTTP port allocation
See also port 2002
RADIUS 1-6, 1-7
TACACS+ 1-6
posture validation
See also NAC
request handling 15-11




Downloaded from www.Manualslib.com manuals search engine

PPP password aging 6-21
privileges
See administrators
processor utilization G-5
profile components
See shared profile components
proxy
See also Proxy Distribution Table
character strings
defining 4-6
stripping 4-6
configuring 4-34
in enterprise settings 4-6
overview 4-4
sending accounting packets 4-7
troubleshooting A-15
Proxy Distribution Table
See also proxy
adding entries 4-35
configuring 4-34
default entry 4-3, 4-34
deleting entries 4-38
editing entries 4-37
match order sorting 4-36
overview 4-34

## Q

quotas
See network access quotas
See usage quotas

## R

RADIUS
See also RADIUS VSAs (vendor specific attributes)
attributes
See also RADIUS VSAs (vendor specific attributes)
in User Setup 7-37
AV (attribute value) pairs
See also RADIUS VSAs (vendor specific attributes)
Cisco IOS C-3
IETF C-14
overview C-1
Cisco Aironet 4-13
IETF
in Group Setup 6-38
interface configuration 3-16
in User Setup 7-38
interface configuration overview 3-11
password aging 6-26
ports 1-6, 1-7
specifications 1-7



Downloaded from www.Manualslib.com manuals search engine

token servers 13-79
troubleshooting A-22
tunneling packets 4-18
vs. TACACS+ 1-6
RADIUS Accounting log
configuring
CSV (comma-separated values) 11-19
ODBC 11-23
configuring CSV (comma-separated values) 11-18
CSV (comma-separated values) file directory 11-16
enabling
ODBC 11-23
enabling CSV (comma-separated values) 11-17
RADIUS user databases
configuring 13-81
group mappings 16-2
RADIUS-based group specifications 16-14
RADIUS VSAs (vendor specific attributes)
Ascend
in Group Setup 6-43
in User Setup 7-43
supported attributes C-31
Cisco Aironet
in Group Setup 6-41
in User Setup 7-41
Cisco BBSM (Building Broadband Service Manager)
in Group Setup 6-51
in User Setup 7-52
supported attributes C-14
Cisco IOS/PIX
in Group Setup 6-40
interface configuration 3-17
in User Setup 7-39
supported attributes C-5
Cisco VPN 3000
in Group Setup 6-44
in User Setup 7-44
supported attributes C-9
Cisco VPN 5000
in Group Setup 6-46
in User Setup 7-46
supported attributes C-13
custom
about 9-28
in Group Setup 6-53
in User Setup 7-53
Juniper
in Group Setup 6-50
in User Setup 7-51
supported attributes C-44
Microsoft
in Group Setup 6-47
in User Setup 7-47
supported attributes C-28
Nortel
in Group Setup 6-49




Downloaded from www.Manualslib.com manuals search engine

in User Setup 7-49
supported attributes C-43
overview C-1
user-defined
about 9-28, D-28
action codes for F-19
adding D-29
deleting D-31
import files D-34
listing D-32
replicating 9-29, D-29
RDBMS synchronization
accountActions table as transaction queue 9-32
configuring 9-41
CSV-based 9-35
data source name configuration 9-37, 9-38
disabling 9-43
enabling in interface 3-6
group-related configuration 9-27
import definitions F-1
log
CSV (comma-separated values) file directory 11-16
viewing 11-18
manual initialization 9-40
network configuration 9-28
overview 9-26
partners 9-39
preparing to use 9-33
report and error handling 9-33
scheduling options 9-39
user-related configuration 9-27
Registry G-2
rejection mode
general 15-5
posture validation 15-11
Windows user databases 15-6
related documentation xxxiii
reliability of network 2-19
remote access policies 2-14
remote logging
See logging
replication
ACS Service Management page 9-2
backups recommended (Caution) 9-10
cascading 9-6, 9-13
certificates 9-2
client configuration 9-17
components
overwriting (Caution) 9-17
overwriting (Note) 9-11
selecting 9-11
configuring 9-21
corrupted backups (Caution) 9-10
custom RADIUS dictionaries 9-2
disabling 9-24
EAP-FAST 10-22
encryption 9-5




Downloaded from www.Manualslib.com manuals search engine

external user databases 9-2
frequency 9-7
group mappings 9-2
immediate 9-19
implementing primary and secondary setups 9-15
important considerations 9-7
in System Configuration 9-21
interface configuration 3-5
IP pools 9-2, 9-45
logging 9-10
manual initiation 9-19
master AAA servers 9-3
notifications 9-25
options 9-11
overview 9-2
partners
configuring 9-23
options 9-12
process 9-4
scheduling 9-21
scheduling options 9-12
selecting data 9-11
unsupported 9-2
user-defined RADIUS vendors 9-9
vs. backup 9-10
Reports and Activity
See also logging
configuration privileges 12-5
configuring 11-20
CSV (comma-separated values) logs 11-13
in interface 1-29
overview 11-6
request handling
general 15-5
posture validation 15-11
Windows user databases 15-6
requirements
hardware 2-2
network 2-4
operating system 2-2
system 2-2
resource consumption G-6
restarting services 8-2
restore
components restored
configuring 8-16
overview 8-16
filenames 8-15
in System Configuration 8-14
overview 8-14
performing 8-16
reports 8-16
with CSUtil.exe D-7
RFC2138 1-7
RFC2139 1-7
RSA user databases
configuring 13-85
group mappings 16-2



Downloaded from www.Manualslib.com manuals search engine

## S

search order of external user databases 15-15
security policies 2-15
security protocols
  Cisco AAA client devices 1-2
  CSRadius G-8
  CSTacacs G-8
  interface options 3-9
  RADIUS 1-6, C-1
  TACACS+
    custom commands 3-9
    overview 1-6
    time-of-day access 3-8
server certificate installation 10-35
service control in System Configuration 11-33
Service Monitoring logs
  See Cisco Secure ACS Service Monitoring logs
services
  determining status of 8-2
  logs
    configuring 11-33
    list of logs generated 11-32
  management 8-17
  overview 1-4, G-1
  starting 8-2
  stopping 8-2
session policies
  configuring 12-17
  options 12-16
  overview 12-16
shared profile components
  See also command authorization sets
  See also downloadable IP ACLs
  See also network access filters
  See also network access restrictions
  overview 5-1
shared secret G-8
shell command authorization sets
  See also command authorization sets
  in Group Setup 6-33
  in User Setup 7-26
single password configurations 1-14
SMTP (simple mail-transfer protocol) G-7
specifications
  RADIUS
    RFC2138 1-7
    RFC2139 1-7
  system performance 1-3
  TACACS+ 1-7
SSL (secure socket layer) 12-13
starting services 8-2
static IP addresses 7-10
stopping services 8-2
stored procedures
  CHAP authentication
    configuring 13-73
    input values 13-66



Downloaded from www.Manualslib.com manuals search engine

output values 13-66
result codes 13-69
EAP-TLS authentication
configuring 13-74
input values 13-67
output values 13-68
implementing 13-60
PAP authentication
configuring 13-73
input values 13-64
output values 13-65
result codes 13-69
sample procedures 13-62
type definitions
integer 13-61
string 13-61
supplementary user information
in User Setup 7-6
setting 7-6
synchronization
See RDBMS synchronization
system
configuration
advanced 9-1
authentication 10-1
basic 8-1
certificates 10-1
privileges 12-4
health G-5
messages in interface 1-29
monitoring
See monitoring
performance specifications 1-3
requirements 2-2
services
See services


## T


TACACS+
advanced TACACS+ settings
in Group Setup 6-2
in User Setup 7-33
AV (attribute value) pairs
accounting B-4
general B-1
custom commands 3-9
enable password options for users 7-35
enable privilege options 7-33
interface configuration 3-7
interface options 3-9
outbound passwords for users 7-37
ports 1-6
SENDAUTH 1-15
settings
in Group Setup 6-2, 6-31
in User Setup 7-22, 7-23
specifications 1-7




Downloaded from www.Manualslib.com manuals search engine

time-of-day access 3-8
troubleshooting A-22
vs. RADIUS 1-6
TACACS+ Accounting log
configuring
CSV (comma-separated values) 11-19
ODBC 11-23
CSV (comma-separated values) file directory 11-16
enabling CSV (comma-separated values) 11-17
enabling for ODBC 11-23
viewing 11-18
TACACS+ Administration log
configuring
CSV(comma-separated values) 11-19
ODBC 11-23
CSV (comma-separated values) file directory 11-16
enabling
ODBC 11-23
enabling CSV (comma-separated values) 11-17
viewing 11-18
Telnet
See also command authorization sets
password aging 6-21
test login frequency internally 8-18
thread used G-6
time-of-day/day-of-week specification
See also date format control
enabling in interface 3-5
timeout values on AAA clients 15-9
TLS (transport level security)
See certification
token caching 1-15, 13-79
token cards
password configuration 1-14
settings in Group Setup 6-18
token servers
ISDN terminal adapters 13-79
overview 13-78
RADIUS-enabled 13-79
RADIUS token servers 13-80
RSA 13-84
supported servers 1-10
token caching 13-79
topologies
See network topologies
troubleshooting
AAA servers A-1
administration issues A-2
browser issues A-4
Cisco IOS issues A-5
database issues A-7
debug logs 11-31, A-14
dial-in issues A-10
installation issues A-16
max sessions issues A-16
proxy issues A-15



Downloaded from www.Manualslib.com manuals search engine

RADIUS issues A-22
report issues A-17
TACACS+ issues A-22
third-party server issues A-19
upgrade issues A-16
user issues A-20
trust lists
See certification
trust relationships 13-9


## U


UNIX passwords D-18
unknown service user setting 7-32
Unknown User Policy
See also unknown users
configuring 15-16
in external user databases 13-3, 15-14
turning off 15-17
unknown users
See also Unknown User Policy
authentication 15-4
authentication performance 15-8
authentication processing 15-8
network access authorization 15-13
posture validation 15-10
update packets
See watchdog packets
upgrade troubleshooting A-16
usage quotas
in Group Setup 6-14
in Interface Configuration 3-5
in User Setup 7-18
overview 1-18
resetting
for groups 6-55
for single users 7-58
user-changeable passwords
overview 1-16
with Windows user databases 13-25
user databases
See databases
User Data Configuration 3-3
user groups
See groups
user-level
downloadable ACLs interface 3-5
network access restrictions
See also network access restrictions
enabling in interface 3-4
User Password Changes log location 11-17
users
See also User Setup
adding
basic steps 7-4
methods 13-3
assigning client IP addresses to 7-10
assigning to a group 7-8




Downloaded from www.Manualslib.com manuals search engine

callback options 7-9
configuring 7-2
configuring device management command authorization sets for 7-30
configuring PIX command authorization sets for 7-29
configuring shell command authorization sets for 7-26
customized data fields 3-3
data configuration
See User Data Configuration
deleting 11-11
deleting accounts 7-57
disabling accounts 7-5
finding 7-55
import methods 13-3
in multiple databases 15-7
listing all users 7-55
number allowed 2-18
number of 1-4
RDBMS synchronization 9-27
relationship to groups 3-2
resetting accounts 7-59
saving settings 7-60
supplementary information 7-6
troubleshooting A-20
types
discovered 15-3
known 15-2
unknown 15-3
VPDN dialup E-2
User Setup
account management tasks 7-54
basic options 7-3
configuring 7-2
deleting user accounts 7-57
saving settings 7-60
Users in Group button 6-54

## V

validation of passwords 8-5
vendor-specific attributes
See RADIUS VSAs (vendor specific attributes)
viewing logs and reports
See logging
Voice-over-IP
See VoIP (Voice-over-IP)
VoIP (Voice-over-IP)
accounting configuration 3-6, 8-21
Accounting log
enabling csv log 11-17
viewing 11-18
enabling in interface 3-6
group settings in Interface Configuration 3-6
in Group Setup 6-4
VoIP (Voice-over-IP) Accounting log
configuring
CSV (comma-separated values) 11-19



Downloaded from www.Manualslib.com manuals search engine

ODBC 11-23

CSV (comma-separated values) file directory 11-16

enabling

ODBC 11-23

VPDN

advantages 2-12

authentication process E-1

domain authorization E-2

home gateways E-3

IP addresses E-3

tunnel IDs E-3

users E-2

VSAs

See RADIUS VSAs (vendor specific attributes)


## W


warning events G-5, G-7

warnings

significance of xxxii

watchdog packets

configuring on AAA clients 4-18

configuring on AAA servers 4-25

logging 11-5

web servers G-2

Windows operating systems

authentication order 15-7

Cisco Secure ACS-related services

services 8-2

dial-up networking 13-10

dial-up networking clients

domain field 13-10

password field 13-10

username field 13-10

Domain List effect 15-7

domains

domain names 13-13, 13-14, 15-6

Event logs G-6

Registry G-2

Windows user databases

See also databases

Active Directory 13-26

configuring 13-30

Domain list

inadvertent user lockouts 13-27

domain mapping 16-9

domains

trusted 13-9

grant dial-in permission to users 13-9, 13-26

group mappings

editing 16-9

limitations 16-4

no access groups 16-7

remapping 16-9

mapping database groups to AAA groups 16-4

overview 13-7

password aging 6-26




Downloaded from www.Manualslib.com manuals search engine

passwords 1-11
rejection mode 15-6
request handling 15-6
trust relationships 13-9
user-changeable passwords 13-25
user manager 13-26
wireless network topologies 2-9



Downloaded from www.Manualslib.com manuals search engine